ERROR 404

¿PREPARADOS PARA UN MUNDO SIN INTERNET?

ESTHER PANIAGUA

Es cuestión de tiempo que la red caiga. ¿Estamos preparados? *Error 404* no es una distopía. Es un impactante ensayo que trata de anticiparse a ella antes de que sea demasiado tarde.

Es cuestión de tiempo que la red caiga. Internet se vendrá abajo y viviremos oleadas de pánico. ¿Suena apocalíptico? No lo es.

En *Error 404*, Esther Paniagua aborda las múltiples formas en las que internet se está cayendo y cómo podría producirse un gran apagón de la red de redes; el caos que ello podría desatar y lo dependientes que somos de ella. Desvela quiénes son los guardianes de internet y nos abre la puerta al lado más oscuro del ciberespacio para hablar de crimen y adicción; de quién convirtió el beicon con huevos en el desayuno estadounidense por excelencia y qué tiene eso que ver con la manipulación; de desinformación, polarización y odio incendiario online; de cómo se ha automatizado la discriminación así como de censura y represión. En definitiva, nos muestra el funcionamiento oculto de una tiranía digital que George Orwell o Aldous Huxley tan siquiera imaginaron.

¿Cómo hemos llegado hasta aquí? ¿Qué se oculta en las tinieblas de internet?¿Hay esperanza de un nuevo amanecer? ¿Seremos capaces de cambiar el rumbo?

Error 404 no es una distopía. Es un impactante ensayo que trata de anticiparse a ella antes de que sea demasiado tarde. Estas páginas analizan los temas de ahora, tan urgentes como cruciales, con una perspectiva crítica y propositiva, pues, tal y como defiende su autora, a pesar de todo aún hay motivos para la esperanza.

Esther Paniagua Gómez

Error 404: ¿Preparados para un mundo sin internet?

ePub r1.0
XcUiDi 25-04-2022

Esther Paniagua Gómez, 2021

Editor digital: XcUiDi
ePub base r2.1




proyecto scriptorium
9
aniversario
"más libros, más libres"
epublibre

Al mañana.
El sol volverá a brillar

«Una llamada urgente y necesaria a reimaginar y rediseñar radicalmente internet por el bien global.»

María Sefidari,
presidenta de Fundación Wikimedia.

«Un diagnóstico clarificador, preciso y sintético del presente como herramienta para crear el futuro. Se lee como una novela.»

Mario Tascón,
socio director de Prodigioso Volcán.

«Un terrorífico relato sobre el fin del mundo, tan preciso y bien documentado que ya nunca volverás a ver internet del mismo modo.»

Toni García, periodista.

«Cuando juntas mentes brillantes suceden cosas brillantes. Pero cuando conectas a Esther Paniagua con las personas que más han cambiado nuestras vidas y el mundo# eclosiona este libro de lectura obligatoria para los que nos proponemos seguirlo cambiando.»

Andreu Vèa,
el biógrafo de internet.

Prólogo

Estamos a tiempo

En 1909, el novelista británico E. M. Forster escribió un breve relato distópico. Se titulaba *La Máquina se para*. En él, describía un mundo inhabitable, reducido a polvo, que había obligado a la gente a vivir bajo la superficie de la Tierra. Cada persona se encontraba aislada en habitaciones dentro de la Máquina, que los dominaba y gobernaba. Esta proporcionaba el sustento y la conexión con el resto del mundo. La gente interactuaba a través de mensajes y hologramas. Todos tenían miles de contactos, pero ninguna relación significativa. El ritmo de vida frenético, en permanente conexión y culto a la Máquina, impedía cualquier vínculo humano profundo. Era una civilización que no conocía el silencio; de fondo estaba siempre el murmullo de la Máquina. Cualquier mínimo comentario en su contra se consideraba una rebelión «contra el espíritu de la época». Una blasfemia.

La Máquina se para fue escrita hace más de un siglo, sesenta años antes de la concepción de internet, pero está de plena actualidad. Las preocupaciones de Forster sobre el futuro de la humanidad —y del planeta— y las consecuencias de la dependencia humana de la tecnología siguen vigentes. Ahora más que nunca. Sus reflexiones sobre la delegación de la voluntad individual, la renuncia a la libertad, el desapego humano, la fractura social o el alcance ilimitado de un sistema que nadie es capaz de entender en su integridad nos conectan hoy con la digitalización y la inteligencia artificial.

La Máquina de Forster es hoy la red de redes, y junto con ella los datos masivos y las tecnologías que sirven para el procesamiento complejo de información (eso a lo que llamamos, erróneamente, «inteligencia artificial»).[*] Esta versión renovada de la Máquina del siglo XXI también se podría parar. De hecho, es una preocupación latente en la comunidad tecnológica y de ciberseguridad. Hay quienes llevan años, y hasta décadas, advirtiéndolo desde diferentes esferas. Así se lo dijo el filósofo y teórico de la conciencia Daniel Dennett al periodista Toni García en 2014: «Internet se vendrá abajo y viviremos oleadas de pánico».[1]

Ese titular fue el origen de este libro, que estaba esperando —en un cajón de mi amigo Toni— a ser escrito. Toni es periodista y escribe libros de gastronomía y cine, pero no le entusiasma el mundo de la tecnología. Yo, como periodista científica, le he dedicado toda mi vida profesional a ella (la tecnología), pero no tenía ninguna intención de escribir un libro. No hasta que Toni me habló de su entrevista con Dennett y de la idea de desarrollar, a partir de la conjetura de la caída de internet, un manuscrito.

Desde ese momento, ya no me pude sacar el tema de la cabeza. Empecé a investigar y me di cuenta de que aquello no solo tenía sentido, sino que era algo que pedía y necesitaba ser contado y transmitido. A medida que me documentaba, se hacía mayor la sensación de urgencia. Todo lo que estaba sucediendo a mi alrededor cobraba sentido bajo el prisma del libro. Pedía a gritos ser escrito.

Luego llegó la COVID-19 y lo cambió (casi) todo. La aceleración de la digitalización y el aumento de la dependencia tecnológica echaron más leña al fuego. No habíamos escuchado las señales de alerta y no estábamos preparados. Ese golpe de realidad hizo más clara la necesidad de concienciar sobre lo que se nos podía venir encima si internet se caía. Como la pandemia, la idea del apagón *online* era cuestión de tiempo. La pregunta no es si pasará, sino cuándo.

Y entonces sucedió algo. Mientras escribía estas páginas, el mundo asistió a varios ensayos a escala milimétrica de lo que podría suceder. El más reciente y sonado fue el incidente que, el 8 de junio de 2021, dejó fuera de servicio a miles de webs en todo el mundo, incluidas las de Amazon, Twitter y Spotify, y periódicos como *El País* o *The New York Times*. La caída se produjo por un error informático en Fastly, el proveedor de servicios de computación en la nube donde se alojan estas páginas. Solo duró una hora, lo suficiente como para acaparar las portadas de los medios de comunicación en todo el mundo.

Unos meses antes le ocurrió a Amazon. Un problema con los servidores de Amazon Web Services (AWS) hizo que multitud de webs se cayeran y dejaran de funcionar aparatos conectados como aspiradoras y timbres de casas.[2] Y en diciembre de 2020 la víctima fue Google: un error por falta de espacio de almacenamiento en sus herramientas de autenticación impidió el acceso a todos los servicios de la empresa, a excepción del buscador.[3] Aquello provocó interrupciones graves que afectaron a muchas empresas, sin capacidad ya para usar el correo electrónico, los sistemas de mensajería instantánea y las plataformas de trabajo en tiempo real. También dejaron de funcionar los dispositivos de Google para el hogar (incluidos termostatos, luces y detectores de humo) y la plataforma YouTube. Todo ello durante los cuarenta y cinco minutos que duró el parón.

Amazon y Google pudieron solucionar el problema con cierta celeridad, pero los sucesos mostraron lo fácil que es provocar un apagón de buena parte de internet, incluso sin pretenderlo. Es el problema de que los servicios *online* estén hoy en día centralizados en tan pocas manos que son siempre las mismas.

Con todo y con eso, la idea —ya no tan teórica— de la caída de internet, con lo que podría comportar y todas sus enseñanzas sobre nuestro nivel de dependencia de la conectividad a escala individual y social, corporativa, gubernamental, administrativa y de infraestructuras críticas, no era lo único que importaba. Importaban, sobre todo, las causas y las consecuencias de dicha dependencia; los riesgos en materia de ciberseguridad; la creciente adicción a estar *online* y al *smartphone* como vehículo de la conectividad; la manipulación y la epidemia de

desinformación; el odio incendiario en redes sociales y la fragmentación y polarización social y política; la automatización de la discriminación; el uso tiránico de los datos personales y de los algoritmos basados en datos masivos; las nuevas formas de trabajo precario vinculadas con plataformas y *apps* digitales; el uso policial de internet; la desigualdad flagrante, la violación de derechos humanos, la censura y la represión; la privatización de la gobernanza y el coste ambiental de la digitalización…

Todo aquello requería de una explicación, de un relato que le diera sentido. Eso es lo que he tratado de hacer en este libro. Pero no solo eso. Como periodista, siempre he defendido el periodismo con propósito como medio para el cambio, y ese es mi lema. Como parte de la escuela del periodismo de soluciones, defiendo que los medios, además de fiscalizar al poder, desvelar corruptelas, fomentar una visión crítica e informar sobre los problemas sociales, deben trasladar a la opinión pública las posibles respuestas y soluciones para hacerles frente. Un periodismo constructivo.

Por eso tenía que contar que también hemos sido capaces, a lo largo de estos años, de usar ese gran invento para cosas maravillosas que jamás habríamos imaginado; que, a pesar de todo, internet, las plataformas digitales, la IA y otras tecnologías conectadas también se usan para el bien; que hacer de estos buenos usos la opción por defecto, esto es, convertir la tecnología en nuestra aliada, es posible. Y tenía que contar cómo podría lograrse aquello o, como mínimo, ofrecer opciones.

Decidí formarme en periodismo científico y tecnológico porque la ciencia, la investigación, es siempre una fuente de buenas noticias: nuevos descubrimientos para mejorar nuestra salud y para conocer mejor al ser humano y el medio ambiente; nuevas tecnologías para llegar donde las personas no podemos, para superar barreras y para tener una vida mejor. Sin embargo, no podía obviar el impacto social negativo de algunas de esas invenciones a través de usos no lícitos o no éticos, o moralmente reprobables. No podía hacer la vista gorda ante las promesas incumplidas de la tecnología.

Ese desencanto, el choque con las sombras del avance tecnológico —que no siempre se traducía en progreso humano—, me hizo comprender la necesidad de volver mi mirada hacia esa cara B. Creó la necesidad de entender más y mejor sus implicaciones y aristas, de poner de relieve lo que sucedía a mi alrededor. También de analizar y tratar de encontrar respuestas para revertirlo.

Este libro tiene un afán didáctico y de concienciación, así como una intención resolutiva. Busca transmitir aprendizajes individuales y colectivos, mostrar una realidad que es siempre más compleja de lo que parece. Intentar hacerla digerible es siempre un riesgo. Hay tantas cosas que contar, tantas interconexiones e interdependencias, tantos matices, frentes, aspectos y ejemplos, que es difícil simplificar, sintetizar y escoger. Por si fuera poco, cada día ofrece nuevos ejemplos de lo que aquí se narra. Es un libro que podría estar en constante crecimiento. El

bucle de documentación y actualización podría ser infinito. ¡No tienen más que observar a su alrededor!

Al contrario que el relato de Forster, *Error 404* no es una distopía. Aspira a anticiparse a ella para estar preparados ante lo que pueda venir. El ejército francés ha contratado a escritores de ciencia ficción para imaginar futuras amenazas.[4] De modo similar, este libro pretende advertir sobre la catástrofe, antes de que sea tarde. No desea criminalizar internet ni renunciar a unas herramientas útiles. No hay nada malo en usar tecnologías que nos facilitan comunicarnos con nuestros seres queridos y conocer a nuevas personas, organizarnos colectivamente, debatir, acceder a información de calidad o realizar gestiones y compras a golpe de clic. Se trata de poner límites y de exigir que estas herramientas sean mejores.

Los desafíos son difíciles, pero están —como mucho— a la altura de enviar al hombre a la Luna, no de viajar más rápido que la luz. Escribo esto desde un optimismo realista, desde el profundo convencimiento de que el cambio es posible y de que las acciones de cada uno de nosotros cuentan (claro está, algunas más que otras). Y lo escribo con la esperanza de un futuro mejor para nosotros y para las generaciones venideras. Para mi hermano Manuel, que acaba de cumplir cuatro añitos.

Primera parte

Oscuridad

Hello darkness, my old friend
I've come to talk with you again
Because a vision softly creeping
Left its seeds while I was sleeping
And the vision that was planted in my brain
Still remains
Within the sound of silence.

Simon & Garfunkel,
«The Sound of Silence»

1

La debacle. Adiós, internet. Bienvenidos al fin del mundo

This is the end, beautiful friend
This is the end, my only friend,
the end Of our elaborate plans, the end
Of everything that stands, the end
No safety or surprise, the end
I'll never look into your eyes again.

Can you picture what will be, so limitless and free
Desperately in need of some stranger's hand
In a desperate land.

The Doors, «The End»

Si una máquina se volviese contra la humanidad e intentase acabar con ella, ¿cómo lo haría? «Yo sé cómo: cargándome internet. No hay manera más sencilla de acabar con nuestro estilo de vida.» La frase de Mo Gawdat,[1] ingeniero de élite y exdirectivo del laboratorio pretendidamente secreto de innovación futurista de Google (Google X), resuena con fuerza.

La idea resulta tan absurda como aterradora. Internet se ha convertido en una parte tan fundamental, tan intrínseca, tan arraigada a nuestras vidas, que lo damos por sentado. Su presencia se ha hecho invisible porque está plenamente integrada en el engranaje del sistema, en su funcionamiento y en nuestras rutinas.

Párense a pensarlo. Gawdat tiene razón. Dependemos tanto de internet que quedarnos sin conexión sería devastador. No hablo de no poder ver vídeos de gatitos o películas en *streaming*, o de jugar *online*, o de hacer videollamadas, o de compartir cualquier cosa en redes sociales. Al menos, no solo. Porque un apagón de internet significaría mucho más que eso. Significaría quedarnos sin un pedazo esencial de nuestro sistema de comunicaciones, de una afectación considerable —cuando no catastrófica— de nuestra infraestructura crítica, de pérdidas económicas millonarias, de adiós al teletrabajo, de falta de suministros y problemas de abastecimiento, de facturas sin pagar, de transporte colapsado, y así hasta el infinito. Tanto que no sabemos hasta qué punto: ni siquiera quienes supuestamente deberían —quienes se ocupan de la seguridad nacional de nuestros gobiernos, o quienes formaron parte de la creación y el desarrollo de internet y siguen implicados en su mantenimiento— pueden decir con certeza qué parte del todo, si no el todo «completo», se vendría abajo junto con la red.

Porque sí, lo de conectarlo todo a internet es muy práctico y tiene un sinfín de beneficios, pero con ellos vienen también sus riesgos. Cuanto más nos conectamos y cuantas más cosas conectamos, más vulnerables somos, y mayor es el efecto dominó en caso de fallo. Porque, siendo así, al desaparecer internet irían cayendo en cascada las piezas que componen el mundo en que vivimos, una parte fundamental del esqueleto del sistema. Así, de un plumazo, fuera de control. Hoy lo tienes todo, mañana te quedas sin nada. Hoy vives en un mundo —más o menos— feliz, mañana en el caos.

¿Suena todo esto a delirio? ¿Hay alguien más preocupado? En realidad, sí. Los gobiernos, las empresas[2] y los propios creadores de la red de redes, a quienes se suman expertos en ciberseguridad y grandes pensadores que llevan años emitiendo señales de alarma. Vinton Cerf,[3] uno de los padres de internet, reconoce que la criatura es altamente vulnerable. El criptógrafo Bruce Schneier alerta sobre los cientos de posibilidades de que algo falle en la red o de que un atacante o grupo de atacantes —sin necesidad de mucho conocimiento ni de recursos— causen estragos. «No es cuestión de si pasará o no, sino de cuándo»,[4] me dijo el filósofo y teórico de la conciencia Dan Dennett en una entrevista para este libro. Años antes se lo soltó a la audiencia del TED 2014 como aperitivo previo a su charla en el trigésimo aniversario de la conocida conferencia:

> Internet se vendrá abajo y cuando lo haga viviremos oleadas de pánico mundial. […] Lo que digo no tiene nada de apocalíptico, puedes hablar con cualquier experto y te dirá lo mismo que yo, que es *cuestión de tiempo que la red caiga*.[5]

«Es cuestión de tiempo que la red caiga.» Dennett lleva años barruntando al respecto. Casi los mismos que su amigo Danny Hillis, que en 2013 se subió también al escenario del TED en Vancouver (Canadá) con una charla titulada «Internet podría estallar. Necesitamos un plan B».[6] Hillis es un científico pionero de la computación e inventor, buen conocedor de la vulnerabilidad y de la fragilidad de la red ante los errores o los ataques:

> Hemos construido este sistema del que entendemos todas sus partes [por separado], pero las estamos usando de maneras muy, muy diferentes al uso esperado y está adoptando una escala muy, muy diferente de esa para la que fue diseñado. De hecho, nadie entiende exactamente todos los usos que se le está dando ahora mismo. Se está volviendo como esos grandes sistemas emergentes; como el sistema financiero, del que hemos diseñado todas sus piezas, pero nadie entiende cabalmente su funcionamiento, todos sus pequeños detalles y qué comportamientos puede tener. […] todo cambia tan rápido que incluso los expertos no saben con exactitud lo que sucede. Nadie sabe realmente cómo es internet ahora mismo, porque es diferente de lo que era hace una hora. Cambia constantemente. Se reconfigura constantemente.

Si pensábamos que la crisis financiera de 2008 había sido un desastre, esperen a ver esto. Porque cuando tomamos un sistema construido básicamente sobre la confianza (llámese sistema financiero o internet), pensado para funcionar a pequeña escala, y lo

expandimos mucho más allá de los límites para los que fue pensado, perdemos el control. No solo el de la propia cosa, sino el de las consecuencias de perderlo; el de lo que pasaría si internet se apagara.

Todo está conectado e interconectado y no sabemos hasta qué punto, ni podemos imaginar las funestas consecuencias de tirarlo abajo. Todo depende de internet. Lo saben en la Internet Society (ISOC), una organización sin ánimo de lucro creada en 1992 para asegurar el desarrollo, la evolución y el uso de internet en beneficio de todos. Una posible caída de internet es una de sus preocupaciones. También le quita el sueño al Oxford Internet Institute (OII), el primer centro para estudiar internet desde una perspectiva multidisciplinar. Como su propio director fundador[7] recuerda, una de las primeras conferencias que organizó el OII se titulaba «¿Se caerá internet?». El tema ha sido una constante entre los asuntos que el selecto grupo trata cada año entre las casi milenarias paredes de la segunda universidad más antigua del mundo.

En realidad, no hace falta teorizar. Como ya avanzamos en el prólogo, tanto en 2021 como en 2020 el mundo asistió a varias muestras muy reales de cómo se puede caer internet, o una buena parte de ella.

CINCO CAMINOS HACIA EL APAGÓN

Entrando de lleno en el escenario de una posible desconexión total de internet, y entendiendo que es teóricamente factible: ¿cómo podría suceder? ¿Durante cuánto tiempo? ¿A qué escala? A los expertos no les interesa dar muchos detalles sobre el tema. Hay continuos ataques a los proveedores de internet que nunca serán confirmados, y será imposible saber qué ha pasado exactamente. A nadie le conviene que salgan a la luz.[8] En efecto, en entrevistas con ex agentes secretos, expertos de ciberseguridad y pioneros de internet, nadie estaba muy dispuesto a profundizar mucho. Aun así, han salido a la luz varios caminos para derribar internet.

Camino 1. Un problema de flow

En menos de treinta minutos todo internet podría caerse. ¿Cómo? A través de un punto débil en el protocolo BGP[*], que rige cómo los datos fluyen en internet. Así lo declaró ante el Senado de Estados Unidos[9] el famoso *hacker* Peiter Zatko, alias Mudge (ahora director de ciberseguridad de Twitter). Él y los otros seis integrantes de su *think tank* de piratas informáticos, L0pht, testificaron el 19 de mayo de 1998, en una audiencia de asuntos estatales sobre seguridad informática.

No era la primera vez que lo hacían. Los ciberexpertos aseguraron haber explicado este riesgo con anterioridad a varios organismos estatales. También declararon que el Departamento de Defensa de Estados Unidos había realizado una gran investigación sobre los posibles ataques contra la infraestructura de internet

usando información proporcionada por L0pht y que, para su disgusto, los hallazgos derivados de ella se clasificaron instantáneamente.

¿En qué consistían estos hallazgos? Entre otras cosas, el grupo L0pht, definido como «estrellas de rock de la élite *hacker*» por *The Washington Post*,[10] había encontrado un fallo en ese protocolo, el BGP. Ese fallo, en el caso de que se alimentara al sistema con información defectuosa, podría desencadenar un efecto en cascada que afectaría a todos los sistemas. Al ser en cascada y automatizado, sucedería relativamente rápido, quizá en menos de treinta minutos. La caída podría durar varios días.

El problema es que, cuando internet llegó a las masas, se abrió un universo de riesgos para los usuarios y para los sistemas e infraestructuras cruciales en el mundo real, incluidas las centrales eléctricas, que se conectaron rápidamente a la red de redes. Internet tiene más de cuarenta años. Aunque la tecnología aún funciona, se le pide que realice tareas que nunca se pretendió que hiciera y para las cuales no fue diseñada de forma segura. No está, por tanto, preparada para ello.

Mudge y el resto de los miembros de L0pht lograron solucionar el error por su cuenta, a pesar de la inacción de los organismos estatales. Sin embargo, su mensaje iba más allá: ellos habían encontrado un punto débil entre los muchos que podrían ser usados para echar abajo internet. En una charla en la conferencia DefCon en San Francisco (Estados Unidos), en 2008, demostró que cualquiera puede hacerlo. Fue tan impactante que la revista *Wired*[11] lo definió como «el mayor agujero de seguridad de internet».

Ese agujero a veces resulta conveniente para las agencias de inteligencia y espionaje de los gobiernos. La agencia de seguridad estadounidense (NSA, por sus siglas en inglés) lo usa para hacer que ciertos flujos de datos sean más fáciles de observar (o, dicho sin eufemismos, para espiar). Así fue como, en 2012, la NSA desconectó por completo a Siria de internet durante algo más de dos días.[12] Esa misma técnica la empleó en 2014 el Gobierno turco para censurar partes de internet.

Otro caso mítico de abuso del protocolo BGP provocó que, en 2010, el 15 por ciento del tráfico de internet pasase durante dieciocho minutos a través de servidores chinos. El operador China Telecom aseguró que sucedió por error, y es posible que así fuera. Otra muestra de lo vulnerable que es el sistema a los errores, y cuanto más a los ataques deliberados.[13]

Hoy estos fallos siguen ahí. Se es más consciente y se invierte más en ciberseguridad, pero el riesgo permanece. Solo en 2017 hubo cerca de catorce mil incidentes de este tipo.[14] Un caso más reciente (2019) sucedió cuando un pequeño proveedor de servicios de internet en Pennsylvania (Estados Unidos) hizo que millones de webs de todo el mundo se desconectaran.[15] La causa principal fue un problema relacionado con el protocolo BGP que afectó a Cloudflare, uno de los principales alojadores de contenido de internet, donde se encontraban las webs afectadas.

Los problemas con este protocolo se llevan tratando de solucionar mucho tiempo, pero el proceso es muy lento y extremadamente difícil. El hecho de que internet pueda caer no ya solo por un ataque intencionado, sino por un error técnico, no es tranquilizador. En cualquiera de los escenarios, sería devastador. Internet se desintegraría.

Camino 2. Los nombres de internet y sus catorce guardianes

Tan peliagudo o más que el del BGP es el problema del Domain Name System (DNS), y hay todo tipo de formas de atacarlo. El DNS es una parte crítica de internet. Es el sistema de nombres de dominio: la nomenclatura de internet, que asigna un nombre a cada participante en la red a nivel global. Permite que estos se conecten fácilmente y da coherencia a la red. Es uno de los fundamentos de internet, lo que diferencia y define a la red de redes frente a otra cualquiera. Por eso, la posibilidad de que se rompa el modelo que mantiene la existencia del espacio de nombres y direcciones único es un verdadero drama. Internet sin DNS es como Correos sin direcciones. Cualquiera podría tener en su casa dos ordenadores que se hablaran, pero que no estuviesen conectados al resto de los ordenadores del mundo.

Pues bien, proteger este sistema, el DNS, es tan importante que hay designados en el mundo catorce guardianes de internet. Su misión es proteger las siete llaves maestras que permiten controlar la red. Siete bombas de relojería que podrían detonar en cualquier momento (aunque activarlas es sin duda complicado). Suena increíble. ¿Cómo es posible que una red global esté gobernada por siete claves controladas por catorce personas? Parece sacado de una película de James Bond.

Uno de esos catorce centinelas, que poco tienen de ficción, es João Damas.**[16]** Es portugués, vive en España y trabaja con sus compañeros en Australia para APNIC, el registro regional de direcciones de internet para la zona Asia-Pacífico. Damas lleva sumergido en las profundidades de internet desde que tiene uso de razón, y conoce la alta vulnerabilidad del sistema. De ahí su cometido como guardián, como parte de un sistema de alta seguridad *offline* que trata de cubrir las carencias de la seguridad *online*.

Cuando se creó el DNS, en los años ochenta, los protocolos eran todo texto y se podía observar el tráfico de todo el mundo. Cualquiera que mirara pasar los datos del cable podía verlo, no estaba encriptado ni había ningún tipo de defensa contra alteraciones. Tanto el DNS como el protocolo BGP son sistemas que forman parte de la base de internet. Es dificilísimo cambiarlos, porque esto implicaría dejar atrás a todo el mundo que está ya conectado. Es decir, desconectar a casi 4.570 millones de personas, el 59 por ciento de la población mundial.**[17]** Vamos, que no es como mudarse de Hotmail a Gmail, o de WhatsApp a Telegram.

Así que lo que han hecho estos guardianes para defender el DNS es crear una capa —protegida por firmas digitales que se renuevan cada tres meses— que al

menos permite preservar los datos contra cualquier alteración mientras están siendo emitidos. Unas llaves físicas, de metal, se usan para controlar el acceso a los ordenadores donde se llevan a cabo las firmas digitales. Su contenido se borraría automáticamente si alguien intentase acceder a ellos sin las llaves.

¿Qué pasaría si se borrasen? Nada en absoluto, porque hay cuatro ordenadores que son copias idénticas de aquellos y que se ubican en dos sitios distintos en Estados Unidos: dos en California y dos en Washington. Para acceder a estos ordenadores hay unas tarjetas de plástico con un chip. Hay siete que activan los ordenadores que están en la costa este y siete los de la costa oeste del país. Damas tiene una de ellas. O, más concretamente, la llave para acceder a una de ellas.

¿Por qué son siete? Respuesta simple: para que haga falta un mínimo de personas que se tenga que poner de acuerdo para corromper el sistema, pero tampoco tantas como para perder el control de quién las tiene. Las tarjetas están guardadas en dos cajas fuertes DeWalt, cada una con siete compartimentos. Cada guardián tiene la llave que abre el cajetín de su tarjeta. Si alguien atacase a los siete guardianes de alguno de los ordenadores, sabría con seguridad su ubicación. Si eso pasase, tendría que resetearse todo el sistema para evitar un mal mayor. Es decir, habría que empezar de cero: vaciar los cajetines, elegir a otros guardianes…

Esto puede pasar en unos días. Mientras tanto, el atacante tiene que poder acceder a la caja fuerte, que está en una jaula, protegida por una combinación. Esta la conocen a medias dos personas que trabajan para la ICANN (Internet Corporation for Assigned Names and Numbers). Esas dos personas saben, cada una, una parte de la combinación. Si se pusieran de acuerdo, podrían conocer el número completo, pero no podrían acceder por sí solas a la caja fuerte; una tercera persona la custodia y tendría que abrirla. Esas dos personas deberían pedir permiso para entrar en el centro de datos donde están la jaula y la caja, notificar que van a ir y qué día y a qué hora, y alguien tendría que autorizarlo. El proceso está fragmentado para que nadie pueda completarlo del todo.

Dada la complejidad del procedimiento, sería realmente complicado un ataque de este tipo contra el DNS. Aun así, no es descartable. A veces las cosas pasan de la manera más tonta. De hecho, Damas confiesa algunos contratiempos. Sin ir más lejos, hubo uno en febrero de 2020, cuando él y los otros seis guardianes de internet se juntaron para actualizar las firmas digitales de los ordenadores que protegen. Su sorpresa fue que no pudieron abrir una de las cajas fuertes. El año anterior el fabricante de las cerraduras de las cajas había advertido que ese modelo —que ya tenía diez años— lo habían dejado de fabricar y que la caja podría fallar. Para evitarlo, se habían comprado ya dos cajas nuevas de reemplazo. En una ceremonia organizada para la ocasión, un cerrajero especializado fue a cambiarlas y una de ellas se bloqueó. Era la última vez que iba a usarse la caja antigua, la última vez que iba a abrirse, pero la casualidad quiso que esa última vez se estropease. «Siempre se ha dicho que las cerraduras solo sirven para mantener fuera a la gente honrada, porque

los demás, si quieren, las fuerzan», pensó Damas después de haber pasado dos días encerrado en el centro de datos con el resto de los guardianes hasta que el cerrajero consiguió finalmente abrir la caja.

Otra forma tonta, o no intencionada, de boicotear el acceso a una buena parte de internet a través del DNS tiene que ver con la base de datos donde están las listas de los diferentes tipos de dominio (.com, .net, .es, .org, etc.) y donde se indica de quién dependen. Si se borra esa base de datos, se tardaría al menos tres o cuatro días en restaurarla. Si el error es menor, puede dar lugar a cortes de acceso de horas y días. No es una mera conjetura: hay precedentes. En 2009, Suecia (en concreto, todas las webs «.se») desapareció de internet por un ridículo error de configuración. Tan tonto como que faltaba un punto al final de cada registro. En España ha habido varios casos similares: en 2006 fue imposible entrar en ninguna web bajo dominio «.es» por un error de actualización de las direcciones DNS de los dominios,[18] y en 2018 un problema técnico en Red.es —la entidad que gestiona los dominios en España— paralizó temporalmente el acceso a las páginas «.es».

Un ataque que aprovechase los fallos de seguridad de IPv6 también sería algo creíble. IPv6 es el nuevo espacio de nombres de internet. Reemplaza al anterior, IPv4, que proveía las direcciones necesarias para identificar y localizar ordenadores conectados a internet. El 3 de febrero de 2011 estas se agotaron: internet se quedó sin números. De ahí que tuviera que pasarse a IPv6. El problema es que tenemos muchísima menos experiencia en la implementación de este sistema que con IPv4. Por tanto, es más vulnerable, y los ciberdelincuentes son expertos en aprovecharlo. En 2018, el ingeniero de redes Wesley George detectó un ataque que estaba aprovechando los puntos débiles de IPv6 para dejar KO un servidor DNS.[19] Aquello fue solo un aviso de lo que los expertos definen como «la próxima ola de apagones *online*».

Camino 3. Apagón «ordeno y mando»

En tiempos de populismo y de autoritarismo *in crescendo*, la censura en y de internet gana adeptos. Los gobiernos la usan como un arma de propaganda… hasta que se vuelve contra ellos y deciden cerrar el grifo.

Puede pasar —y ha pasado— que un Gobierno decida impedir el acceso a internet, o a algunas de sus partes. Los ejemplos son numerosos. Este mismo 2021, el Gobierno de la India bloqueó el acceso a internet en varios distritos de un estado fronterizo con Nueva Delhi, la capital del país, en un intento por reprimir las protestas contra las reformas agrícolas en el país.[20] Por su parte, el nuevo Gobierno militar de Birmania —que accedió al poder tras un golpe de Estado— bloqueó el acceso a Facebook, que es allí la puerta de entrada a internet para la mayoría de las personas.[21]

En el verano de 2013, la sociedad turca organizó una serie de protestas masivas por todo el país en respuesta a la acción violenta del Gobierno contra unos manifestantes ecologistas. Su principal medio de información y organización fueron las redes sociales. Ese fue el detonante para que, en 2014, el Gobierno turco legalizase la censura en internet, cuyo acceso estaba ya muy restringido. En esa fecha, los activistas pro derechos humanos calculaban que las autoridades habían cerrado el acceso a más de cuarenta mil cuatrocientas webs. La forma de materializar esa censura, mencionada antes, fue a través del protocolo BGP.

Más grave fue lo que pasó en la Cachemira india. En pleno 2019, el Gobierno apagó internet durante siete meses. Fue la desconexión de mayor duración en una democracia, y sus efectos todavía colean. Como relata la periodista Pavithra Mohanlong en *Fast Company*,[22] el 5 de agosto de 2019 el Gobierno indio cortó todas las líneas telefónicas y las conexiones a internet en la región sin previo aviso. Ausencia de comunicación, hilos de WhatsApp silenciados, facturas no pagadas, opositores detenidos, libertad de movimientos restringida y carreteras cerradas y patrulladas por decenas de miles de soldados armados fueron solo algunas de las consecuencias. «No sabíamos lo que estaba sucediendo […]. Fue bastante difícil durante los primeros quince días porque no hubo comunicación y la gente no pudo moverse porque había toque de queda», le contó un ciudadano cachemir a la periodista. Incluso después, cuando pudo regresar a su oficina, no pudo comunicarse con las personas de su organización. Por supuesto, el apagón afectó también a las empresas y a la economía de la India. Se estima que las pérdidas fueron de unos 2.300 millones de dólares.

India encabeza la lista mundial de países con mayor número de apagones de internet impuestos por gobiernos locales, estatales o nacionales.[23] Solo en 2018, el servicio de internet se cortó ciento treinta y cuatro veces en el país asiático. Su competidor más cercano es Pakistán, donde se cerró internet doce veces en 2018.

En Egipto también pasó durante la Primavera Árabe (20102012). Tras décadas de un Gobierno autoritario, miles de personas se organizaron a través de las redes sociales para manifestarse en la plaza Tahrir de El Cairo y reivindicar la democracia. La respuesta del Gobierno fue ordenar a las compañías de telecomunicaciones que cortaran el acceso a internet, las llamadas de voz y los SMS. También obligó a dichas empresas a enviar mensajes de propaganda a favor del régimen.

El cierre de internet en Egipto duró cinco días. Hay otros que son permanentes, como en Corea del Norte, donde, a pesar de haber conexión, el Gobierno no permite acceder a ella a la mayoría de la población. En China no se pueden usar Google, WhatsApp, Facebook y otras redes sociales. En Rusia, por su parte, ya han empezado a prepararse para un posible apagón. En diciembre de 2019 concluyó con éxito su primera prueba de desconexión de la red global.[24]

Otra cosa que puede pasar —y que también ha pasado— es que haya algún fallo en el intento de cortar el acceso a internet. El domingo 24 de febrero de 2008 usuarios

en todo el mundo se quedaron sin YouTube durante más de dos horas. La causa: Pakistán cometió errores al tratar de bloquear el acceso de los usuarios de internet en el país por orden del Gobierno. Este no tenía la intención de que la censura afectase a todo el planeta, pero así fue. Debido al modo en que funcionan los protocolos de internet, esta acción resultó en el secuestro del tráfico de YouTube a escala global. Es la típica caída que puede tener lugar hoy perfectamente: el «efecto mariposa» de internet. Y fue un accidente, pero podría ser intencionado.

Más hipotética es la posibilidad de que un solo Gobierno tire abajo toda la red de forma intencionada. La idea de que algo así suceda se usa —especialmente desde Estados Unidos— contra la iniciativa china del 5G, el nuevo estándar global de comunicación inalámbrica. Lo que dicen los teóricos de esta posibilidad es que, si el 5G del gigante chino Huawei es adoptado ampliamente, dará control al país asiático sobre los recursos de telecomunicaciones subyacentes. El Gobierno de Xi Jinping podría controlar toda esa infraestructura y apagar de forma remota al menos ciertas partes de internet, o venderla (deshaciéndose de Huawei) al mejor postor. La pregunta es: ¿por qué demonios lo harían? Podrían usarlo como amenaza, pero no tendría sentido materializarlo. China depende del comercio global. Sería como dispararse en el pie.

Además, lo de apagar internet no sale gratis. Un informe de Top10VPN reveló que hubo doscientos veintiséis apagones «ordeno y mando» «importantes» en cuarenta países entre 2019 y abril de 2021.[25] Estos costaron un total de 14.400 millones de dólares a la economía mundial, con su mayor impacto en Oriente Próximo, África, Asia, Irak, Sudán e India.

Camino 4. Continente sin contenido

En sus comienzos, cuando internet era una red de comunicación entre pares (dos nodos cualesquiera), era más resistente porque estaba descentralizada. Ahora, si bien los protocolos de internet siguen siendo distribuidos, dependemos cada vez más de recursos centralizados. Es lo que se conoce como «consolidación», es decir, la reducción del número de actores en el mercado y la concentración en solo unos pocos, pero muy grandes, que controlan las aplicaciones de internet, la provisión de acceso y la infraestructura de servicio. Por ejemplo, antes un periódico establecía comunicaciones directamente con el ordenador de otra persona, empresa o universidad, alojándose en un proveedor local, muy cercano a los dos extremos de la red, que son el periódico y sus usuarios. Ahora lo hace en una de las grandes plataformas de distribución de contenido —Akamai, AWS (Amazon Web Services), Fastly o Google— que copan el mercado y que están normalmente muy alejadas de los dos extremos de la comunicación. Una de las consecuencias más graves de todo esto es que, si hay un ataque a alguna de esas plataformas, se caerá todo lo asociado a ellas. Periódicos, todo tipo de webs, plataformas de *streaming*… Poco queda fuera de

su alcance, como pudimos comprobar con la caída masiva de webs asociada a un error informático de Fastly.

Mientras que antes había varios buscadores, ahora «googlear» es un verbo. Esto crea puntos únicos en los que se puede crear una ruptura, es decir, usarlos para interrumpir o bloquear un servicio. Estamos poniendo todos los huevos en la misma cesta por las ansias de inmediatez y de disponibilidad permanente de los datos en tiempo real.

Un ataque contra Google o contra alguna de las plataformas de distribución de contenido como AWS tendría un impacto considerable, como ya hemos visto.

Camino 5. Ataque móvil

¿Y si el ataque se ceba con nuestros inseparables teléfonos inteligentes? No sería algo trivial, ya que los celulares están reemplazando a los ordenadores como principales dispositivos de acceso a internet. Ya en 2018, un 58 por ciento de las visitas a la web a escala mundial se hicieron desde el móvil.**[26]**

Es fácil interferir en las comunicaciones celulares, porque el medio en el que viajan, el aire, es compartido. Puede llegar cualquiera con una emisora básica en la banda de los teléfonos móviles y emitir tal ruido, tal cantidad de interferencia, que deje de funcionar todo ese sistema en, por ejemplo, una ciudad entera.

DE LA SUPERNOVA A LA SUPERINTELIGENCIA

Hasta ahora hemos visto una serie de métodos prácticos para una desconexión de internet. Quería comenzar presentando formas muy reales en las que internet puede fallar o en las que se puede derribar la red. Pero no quiero negar a los lectores la posibilidad de explorar otras ideas más locas: una dosis de ciencia ficción improbable.

Históricamente ha habido predicciones de apagones de internet de forma regular. Una de las más famosas es la de Bob Metcalfe, el inventor de *ethernet*, la tecnología de red que conecta los ordenadores entre sí y a internet a través de cables. Metcalfe tenía una columna llamada «Desde el éter» en la revista *InfoWorld*, de la que era editor. En el número del 4 de diciembre de 1995**[27]** afirmó: «Internet pronto se convertirá en una supernova espectacular y en 1996 colapsará catastróficamente». Además, identificó una serie de factores que provocarían el colapso de internet, incluidas las brechas de seguridad, las sobrecargas de capacidad y la demanda de vídeo en línea.

Como ya sabemos, su predicción no se cumplió, y decidió comerse —literalmente — sus palabras.

En un acto que él mismo definió como su «mayor truco publicitario de todos los tiempos», arrancó su columna de *InfoWorld*, la rompió en pedazos y los introdujo en

una licuadora eléctrica con agua. Luego puso el contenido en una taza y lo sorbió.

Unos años antes de Metcalfe, en 1991, el experto en ciberseguridad Winn Schwartau usó el término «Pearl Harbor electrónico» en su declaración ante el Congreso de Estados Unidos. Schwartau describió un ataque «devastador» que causaría estragos en la sociedad en general, un evento «verdaderamente paralizante», que provocaría «daños masivos» a una escala que socavaría el orden y el funcionamiento de la sociedad tal y como la conocemos. La idea ha seguido resonando. Fue repetida en el Congreso estadounidense en sucesivas ocasiones y en boca de diferentes ponentes. También Richard Clarke, ex coordinador nacional de Seguridad, Protección de Infraestructura y Antiterrorismo de Estados Unidos, alertó de esta posibilidad en la conferencia Safenet 2000 el 8 de diciembre de 2000. En 2011, el ex secretario de Defensa de Estados Unidos Leon Panetta advirtió al Senado estadounidense sobre la «posibilidad real» de un próximo Pearl Harbor en forma de ciberataque que podría paralizar la red eléctrica, internet, las telecomunicaciones, los sistemas de seguridad y financieros, etc. En 2012 volvió a repetirlo, alegando que tal acción podría ser tan destructiva como el ataque terrorista del 11-S, causar pánico, destrucción e incluso la pérdida de vidas, detener y conmocionar a la nación, así como crear un nuevo sentido profundo de vulnerabilidad.

Hay otros escenarios poco plausibles, algunos no enteramente descartables y otros que rozan el delirio. Hemos visto antes desconexiones intencionadas en que gobiernos autocráticos deciden cerrar o bloquear el acceso a cualquier plataforma de conocimiento y de libre expresión *online*. También por iniciativa propia de los gobiernos, pero por motivos muy diferentes, podría darse una forma de apagón preventivo, ante la amenaza de control *online* de la infraestructura de uno o varios países, o ante una ciberguerra que haga que otros decidan desconectarse. Podría, hipotéticamente, suceder que un grupo de *hackers* maliciosos organizados a escala mundial decidiera cargarse internet «por el bien de la humanidad»; o que un virus informático obligara a los usuarios de todo el mundo a desconectarse por riesgo de infección; o que la sociedad civil organizada —harta de la vigilancia, la manipulación y el control de internet llevados al extremo, unidos al aumento de la desigualdad y a la precarización de la vida y el trabajo— se rebelara contra la red de redes en una especie de toma de la Bastilla del siglo XXI; o que una concatenación de efectos inesperados e indeseados en el uso de sistemas inteligentes provocara el apagón; o que un ataque de pulso electromagnético o una enorme llamarada solar como la que impactó en la Tierra hace ciento sesenta años nos golpeara de nuevo y destruyera nuestras redes eléctricas, comunicaciones satelitales e internet; o, como dicen los apóstoles de la singularidad tecnológica, que una superinteligencia nos dominara y decidiera acabar con internet ante la posibilidad de que lo usemos como arma contra ella; o que esta superinteligencia se cargara la red de redes, actuando de buena fe, bajo la consideración de que internet es malo y de que su deber moral para protegernos es crear uno nuevo, liberado de todo lo que hacía «malo» al anterior.

Hablando de «superinteligencia», y por muy novelesca que pueda parecer esta última hipótesis, hay quienes creen que es más que factible que esta acabe con internet y que James Cameron podría acercarse peligrosamente a la realidad con la Skynet de *Terminator* (esa tecnología que se hace autoconsciente y decide atacar a la civilización ante el temor de ser desactivada). Creen estos «singularitarios» apocalípticos que, tarde o temprano, la inteligencia artificial (IA) será capaz de crear otra superior a la humana. Mo Gawdat pertenece a este club, abanderado por empresarios conocidos como Elon Musk (fundador de Tesla) o por expertos como Nick Bostrom, un prominente filósofo que dirige el Instituto para el Futuro de la Humanidad (FHI, por sus siglas en inglés) de la Universidad de Oxford. Incluso científicos como Stuart Russell, pope de la inteligencia artificial, se han subido al carro con su corto *Slaughterbots*,[28] en el que muestra un plausible futuro cercano en el que ejércitos de microdrones autónomos atemorizan a la población con ataques asesinos dirigidos a personas concretas o a grupos seleccionados. Todos ellos han advertido de alguna manera del riesgo de una extinción de la humanidad a manos de máquinas autónomas dotadas de inteligencia artificial con cierto grado de sofisticación. Dicen que «todo lo que vemos en las películas de ciencia ficción va a pasar».[29]

La realidad a menudo supera a la ficción, y las cosas podrían ponerse muy mal si realmente hay un apagón. Lo veremos en el siguiente capítulo.

2

A cuatro comidas del caos

La noche es más oscura justo antes del amanecer. Y, os lo prometo, está a punto de amanecer.

CHRISTOPHER NOLAN (dir.), *El caballero oscuro*

El 1 de septiembre de 1859 la Tierra fue sacudida por una monumental tormenta solar nunca antes vista. Es lo que se conoce como el «evento Carrington». La enorme llamarada solar impactó en el planeta en plena revolución del telégrafo, al que dejó temporalmente sin servicio, aunque sin causar grandes estragos. Hoy, más de ciento sesenta años después, podría ser devastador. Ese efluvio del Sol podría dejarnos, paradójicamente, sin luz y, por supuesto, echar abajo internet. Es decir, cargarse todo aquello en lo que se sustenta y de lo que depende la vida actual.

El evento Carrington supuso un hito, pero no fue algo ni tan excepcional ni tan aislado: una tormenta magnética similar podría golpearnos de nuevo. Hasta ahora se creía que no había tenido lugar un evento de este tipo tan extremo, pero se han encontrado pruebas[1] de otro de mayor alcance que afectó al este de Asia en 1770, casi noventa años antes. Algo que se ha descubierto gracias a registros estatales y diarios personales de habitantes de Corea, China y Japón en aquella época, que han permitido reconstruir lo que sucedió.

Por lo que se sabe, esta fue la tormenta geomagnética registrada más larga de la historia. Duró al menos nueve noches, no dos, como el evento Carrington. Y eso no es todo: otros documentos históricos podrían conducir al descubrimiento de eventos geomagnéticos aún más prolongados.

En efecto, las observaciones históricas advierten de que esto puede ser algo que ocurre con más frecuencia (cada pocas décadas). Por tanto, podría ser una amenaza más inminente para nuestra civilización. Dicho de otro modo: solo es cuestión de tiempo que asistamos a una de estas verbenas solares. Hasta ahora hemos tenido suerte. En 2012, una poderosa erupción solar atravesó la órbita terrestre. Afortunadamente, la Tierra no estaba allí en ese momento. Si hubiera ocurrido una semana antes, el planeta que habitamos habría estado en la línea de fuego.

Las consecuencias habrían sido comparables a un choque de un asteroide lo bastante grande como para hacernos retroceder a niveles del siglo XVIII. Una «fiesta» geomagnética de esa clase provoca una rápida caída de la fuerza del campo magnético de la Tierra; una alteración que hoy tendría consecuencias como apagones de amplio alcance que inutilizarían las redes eléctricas y que provocaría

interrupciones en las comunicaciones o interferencias con las señales de navegación del GPS.

Un informe de 2008 del Consejo Nacional de Investigación de Estados Unidos[2] (NRC, por sus siglas en inglés) calculó que el impacto económico de un evento como el Carrington en pleno siglo XXI podría ser de hasta dos billones de dólares durante el primer año, con tiempos de recuperación de hasta diez años. Es decir, más del total de la economía española, que en 2019 no alcanzó los 1,3 billones de euros (algo más de 1,5 billones de dólares).

Ahora, el impacto económico sería mayor, al igual que la brecha con cualquier producto interior bruto (PIB), dado el impacto del coronavirus. Hablando de la COVID-19: se estima que el PIB de la zona euro cayó un 6,8 por ciento en 2020, y un 6,4 por ciento en la Unión Europea.[3] En Estados Unidos, la economía se contrajo un 3,5 por ciento anual en 2020, la mayor contracción desde la desmovilización tras la Segunda Guerra Mundial en 1946.[4] Nada, pues, comparado con una disminución potencial de cerca de un 14 por ciento del PIB[5] que podría provocar una tormenta solar geomagnética severa.

No tan extremas, pero con consecuencias nada desdeñables, han sido otras tormentas geomagnéticas más recientes. Una de ellas se conoce como el «evento Halloween». Sucedió a principios de noviembre de 2003 y se calcula que fue significativamente más débil que el evento Carrington. Sin embargo, eso no impidió que causara problemas en transformadores eléctricos del norte de Europa y apagones posteriores, además de reenrutamientos de vuelos, cambios en casi un 60 por ciento de las misiones espaciales e impactos de diferente calado en las industrias sensibles al clima espacial. También es conocido el evento solar que colapsó la red eléctrica de Quebec en 1989. El apagón general duró más de nueve horas y afectó a más de seis millones de personas.

Los expertos reconocen, sin embargo, que apenas tienen capacidad para pronosticar eventos extremos de este tipo. Hasta el momento, el impacto de una llamarada solar en la Tierra solo se puede predecir con una precisión de entre seis y doce horas.[6] Considerando que el impacto podría producirse en unas quince horas, el margen es mínimo.

También han sido escasamente documentados y comprendidos los posibles efectos económicos y sociales de los cortes de sistemas tecnológicos críticos que desencadenarían tales acontecimientos. En la práctica, podríamos titularlo como «de vuelta a la Edad de Piedra» o, cuando menos, a hace unos cuantos siglos.

LÍMITE: CUARENTA Y OCHO HORAS

Centrémonos en las consecuencias de un evento al estilo Carrington. En específico, de un apagón eléctrico. ¿Cuán terrible podría ser algo así? ¡Realmente terrible! Incluso aunque fuera algo a menor escala, sería un dolor de cabeza importante. Es un

efecto dominó: comienza siendo una molestia y pasa a ser un caos cuando empieza a cundir el pánico.[7] Todo se vuelve una competición: por la comida, por los medicamentos, por la gasolina. Se producen saqueos, peleas, asesinatos, guerras entre bandos. Es una cuestión de supervivencia. Si el *shock* estuviera más localizado, de inmediato se habilitarían medios para que llegasen recursos desde otras partes del país. El gran problema sería que pasase a escala nacional, en España, o que se extendiese por Europa, ya que los sistemas están interconectados.

Como ejemplo podríamos mencionar el «apagón europeo de 2006». El detonante fue una desconexión intencionada de una línea de alto voltaje en el norte de Alemania para dejar pasar un barco por debajo. Esto condujo a la sobrecarga de las líneas, que dividió a la red en zonas y condujo finalmente a la desconexión de millones de clientes en Alemania y en Francia, así como a cientos de miles en Bélgica, Países Bajos, Italia y España, que se quedaron sin electricidad.

¿Qué ocurre cuando pasa algo así? Como explica Fernando Sánchez, director del Centro Nacional de Protección de Infraestructuras y Ciberseguridad de España (CNPIC), cuando hay un incidente resulta clave la coordinación a escala nacional e internacional, pero quienes tienen que resolver la crisis son los operadores. Cuanto más tiempo esté un servicio sin funcionar, más tardará este en regenerarse. Es decir, a mayor ínterin, más consecuencias. Cuando cae un sistema, recuperarlo no es fácil. Si se ha quemado un transformador eléctrico, tal vez hagan falta meses para que llegue uno nuevo de la fábrica, que puede estar en otro país. Si se para una central nuclear, esta tarda días en volver a producir electricidad. Ponerla de nuevo en marcha no es solo cuestión de pulsar un interruptor, requiere tiempo.

A partir de ahí se activa un círculo vicioso de interdependencias con consecuencias en cascada. Si te quedas sin luz te quedas sin combustible, y sin combustible no puedes alimentar una central. Estamos ante un tema muy complejo, porque nuestro sistema de organización lo es. Este es como un reloj suizo, en el que todo funciona perfectamente, donde cada componente de la sociedad ejecuta un trabajo determinado. Si uno de ellos se viene abajo, tenemos serios problemas. Si lo que se viene abajo es la electricidad, tenemos un fallo multiorgánico.

Se considera que cuarenta y ocho horas es el plazo límite para el caos en el paso de un estado de normalidad a otro de crisis. Como le gusta decir al Servicio de Seguridad del Reino Unido, el MI5, «estamos a cuatro comidas de la anarquía». A cuatro comidas del caos. Podemos quitarnos capas de comodidad, pero en el momento en que no tenemos acceso a los alimentos, a los medicamentos vitales o al agua, ya solo se trata de mantenerse con vida a toda costa.

El saqueo se intensifica a medida que se prolonga el apagón y la gente se queda sin estos bienes básicos y se frustra cada vez más. Los brotes de robos se hacen cada vez más frecuentes. Los delincuentes explotan la falta de sistemas de iluminación y seguridad, además de la sobrecarga de unas fuerzas policiales que no dan abasto.

La imposibilidad de acceder a los servicios básicos eleva el malestar social y físico. A los problemas de agua contaminada y de suministro de alimentos se unen las dificultades en el uso de equipos de atención médica en el hogar, el aumento del ruido, la contaminación y otros factores que incrementan el número de muertes.

Como lo describe un informe del Centre for Risk Studies de la Universidad de Cambridge realizado para la firma británica Lloyd's of London:[8] los proveedores de datos y servicios de telefonía móvil dejarían de funcionar al acabarse las baterías de respaldo y el combustible para los generadores. Solo funcionarían los generadores diésel, que mantendrían activos los servicios telefónicos de emergencia. Por supuesto: adiós, internet.

En un principio las empresas, los hospitales y las instalaciones públicas con generadores alternativos podían seguir funcionando, pero por un tiempo limitado. Todas las formas de sistemas de comunicación sin fuentes de alimentación alternativas se verían obstaculizadas por fallos eléctricos. Fuera señales de tráfico, luces en las calles, ascensores, vagones de metro, comida refrigerada o congelada y cualquier bien que requiriese refrigeración.

Se sucederían los accidentes industriales, y con probabilidad habría problemas de tratamiento de aguas residuales y contaminación del suministro. La mayoría de las personas ni siquiera podría tirar de la cadena del inodoro, porque el suministro de agua urbana depende en gran medida de bombas eléctricas. Esto no bloquearía del todo la distribución, pero sí la limitaría. El agua seguiría llegando a gran parte de los hogares por la inercia de la gravedad desde los depósitos. Sin embargo, en edificios con más de seis o siete plantas se requerirían generadores para los usuarios instalados en la sexta y las superiores.

Por descontado, se produciría también una disminución drástica de la productividad empresarial a medida que se cerrasen los lugares de trabajo. Y sería cada vez más difícil —si no imposible— desplazarse a los que siguieran abiertos. Los atascos, sin señales de tráfico en funcionamiento, serían gigantescos. Un gran número de estaciones para repostar dejaría de estar operativo en poco tiempo.

También se interrumpirían los servicios ferroviarios. Los autobuses de reemplazo no serían muy efectivos, debido a los atascos y, de nuevo, a la falta de gasolina. Sin transporte público ni alimento para sus motores, no habría manera de moverse que no fuera a pie o por medios mecánicos. El transporte por aire dejaría de funcionar igualmente. Los aeropuertos se verían obligados a cerrar por no tener energía para los equipos de inspección de seguridad y de verificación electrónica de los pasajes, entre otros graves riesgos de seguridad.

El comercio también quedaría tocado con la suspensión de las operaciones portuarias y la interrupción de las exportaciones e importaciones. Habría un alto en la producción con un enorme impacto en cascada a lo largo de la cadena de suministro.

El consumo sufriría de igual modo. Tras el primer día de compras compulsivas, la imposibilidad de pagar por medios electrónicos y la escasez de cajeros automáticos

con servicio mantendrían bajos los niveles de consumo.

El apagón provocaría el cierre de fábricas y la interrupción de la actividad comercial, responsables de un alto porcentaje de la producción económica del país. El impacto económico implicaría daños directos a los activos y a la infraestructura, una disminución de los ingresos por ventas a las empresas de suministro de electricidad, una pérdida de ingresos por ventas a las empresas y una paralización de la cadena de suministro. Se perderían miles de millones de euros en cuestión de días. En total, cerca de un 5 por ciento del PIB.

RIESGO EXPONENCIAL

De vuelta a la realidad y fuera de abstracciones como una posible tormenta solar geomagnética, que parece casi cuestión de suerte, encontramos riesgos más reales. Amenazas que también supondrían apagones eléctricos generalizados y, por tanto, desactivarían todas las formas de alta tecnología y echarían abajo internet.

No son amenazas naturales, sino creadas por el ser humano. Tal vez la más devastadora sería un ataque de pulso electromagnético (EMP, por sus siglas en inglés). Mucho se ha especulado sobre este tipo de explosión nuclear que desactivaría prácticamente todos los dispositivos electrónicos y transformadores eléctricos a su alcance y que causaría daños duraderos en las infraestructuras críticas.

Todo Estados Unidos (o incluso varios países) podría quedarse en la oscuridad absoluta ante un evento u ofensiva de este tipo. Y eso entre otras graves consecuencias, dado que la electrónica se utiliza hoy para controlar, comunicar, computar, almacenar, administrar e implementar casi todos los aspectos de los sistemas civiles. Estos sistemas también dependen de internet, que, obviamente, en este contexto no funcionaría.

Los efectos colaterales serían incendios inducidos, descargas eléctricas, paralización del transporte y los sistemas de apoyo esenciales (como hospitales, plantas de energía nuclear e instalaciones químicas). Es decir, se ponen en riesgo todos los sectores de infraestructura crítica. Su naturaleza interdependiente complicaría, además, el impacto del evento y la recuperación posterior. Esto implicaría paralizar la economía estadounidense y su ejército.

La omnipresente dependencia del sistema de energía eléctrica invita a países rivales a aprovechar esta vulnerabilidad. Consciente de ello, el Congreso de Estados Unidos creó en 2001 la Comisión EMP para evaluar los riesgos y efectos de un atentado de este tipo, con varios países candidatos a liderarlo: China, Rusia, Corea del Norte, Irán y, potencialmente, Pakistán. Donald Trump, durante su presidencia, fue consciente de que sus crecientes rivalidades y tensiones con estos países aumentarían los riesgos de un ataque, y, en marzo de 2020, firmó un decreto presidencial para preparar al país con vistas a mejorar su prevención y recuperación ante un suceso así.

Existe, sin embargo, un riesgo más inmediato y creciente que el de un ataque

EMP, que, además, internet facilitaría: un ciberataque contra la red eléctrica. Es algo, desde luego, más sencillo de perpetrar que un ataque de pulso electromagnético, pero con efectos similares (a menor escala). ¿Qué pasaría si alguien —pongamos, un pirata informático— usase internet para cortar la electricidad y, de paso, desconectar la red? Sobre ello especulaba ya en 2015 el informe de la Universidad de Cambridge para Lloyd's. Los motivos del encargo son obvios: un mercado de seguros necesita estar preparado para todo tipo de eventualidades. Comprender el impacto de sucesos graves es crucial para las aseguradoras en un ámbito con un nivel significativo de incertidumbre. En específico, la realización del estudio de un posible apagón energético pretende servir de guía para el desarrollo de coberturas de riesgo cibernético.

El documento se centra en los posibles impactos de un hipotético apagón eléctrico derivado de un ciberataque que podría sumir a quince estados de Estados Unidos en la oscuridad y dejar a noventa y tres millones de personas sin electricidad. La hipótesis es esta: un grupo de individuos no identificados contrata los servicios de una serie de programadores moralmente dudosos que sabe cómo penetrar en los sistemas de red del sector eléctrico nacional. Estos instalan un programa malicioso (o *malware*) en el sistema, que permite enviarles información desde dentro de la red y también recibir comandos. El *malware* permanece inactivo mientras los atacantes se preparan para el día D, cuando se produce el apagón.

¿Suena poco creíble? «El escenario, aunque improbable, es tecnológicamente posible», aseguraban los autores en el informe, publicado en julio de 2015. Cuatro meses después sucedió en Ucrania.

Todo comenzó en Crimea. En noviembre, casi dos millones de crimeos se quedaron sin electricidad y en la oscuridad, pero no veinticuatro o cuarenta y ocho horas, sino durante dos semanas. Si bien el servicio de energía fue restaurándose paulatinamente días después de iniciarse el corte eléctrico, el acceso a la electricidad siguió siendo restringido e intermitente, limitado a algunas horas al día y solo en las ciudades (no en las zonas rurales), hasta que se lograron restablecer los suministros. Se declaró el estado de emergencia, la internet por cable y móvil dejaron de funcionar, con una marcada escasez de redes móviles —siquiera para llamadas a servicios esenciales como ambulancias y bomberos—, y se interrumpió el suministro de agua en edificios de gran altura.

Los residentes de la península de Crimea tuvieron que aprender a vivir con refrigeradores de descongelación, tiendas vacías, carreteras oscuras y escuelas cerradas, con el zumbido constante de los generadores que llenaban las calles, incapaces de abastecer adecuadamente a los hospitales de Crimea y mucho menos a las empresas, la mayoría de las cuales se vieron obligadas a cerrar.

A pesar de la resiliencia y la aparente calma de los crimeos, acostumbrados a periodos de escasez, la frustración fue *in crescendo*. A los problemas anteriores se

unieron los de transporte: tranvías detenidos y semáforos apagados, saturación en las únicas estaciones de servicio abiertas, calles y carreteras en total oscuridad.

El apagón de Crimea no se debió a un ciberataque, sino a un ataque físico contra varias subestaciones, pero el que se produjo en Ucrania menos de un mes después sí fue obra de los *crackers*[*]. Ese ataque —y otros posteriores— se consideró una represalia por la ofensiva que causó el apagón en Crimea a manos de activistas proucranianos que estaban en desacuerdo con la adhesión a Rusia de este territorio reclamado por Ucrania.

El ciberataque contra la red eléctrica ucraniana es conocido como la primera acción exitosa de este tipo. El *modus operandi* en este caso de craqueo eléctrico por vía informática fue el de la intrusión cibernética remota en tres compañías regionales de distribución de energía eléctrica. Los cortes de luz afectaron a unos doscientos veinticinco mil residentes en múltiples instalaciones centrales y regionales (con casi sesenta subestaciones desconectadas y algunas fuentes de alimentación alternativa deshabilitadas también por los atacantes).

El ciberataque se sincronizó y se coordinó probablemente después de un extenso reconocimiento de las redes de las víctimas. Se cree que los atacantes habían conseguido con antelación credenciales legítimas para facilitar el acceso remoto. También se detectó la presencia del programa maligno BlackEnergy en empresas ucranianas en sectores de infraestructura crítica.

En 2016 hizo su aparición en escena el destructor de industrias Industroyer, un programa maligno que algunos analistas califican como la «mayor amenaza para los sistemas de control industrial desde Stuxnet»[9] (de este otro hablaremos más adelante). También conocido como CrashOverride, se trata de un *malware* diseñado para echar abajo la electricidad en ciudades enteras aprovechándose de las debilidades de sistemas industriales anticuados.

La diferencia fundamental de este sistema en comparación con el usado en 2015 era que, mientras que el primero requirió de manipulación manual a través de inicios de sesión remotos para controlar las estaciones de trabajo del sistema, el segundo codificó dicha manipulación dentro del *software*. Es decir, en lugar de cortar el flujo de electricidad seleccionando los objetivos uno por uno, este sistema permitía automatizarlo y, por tanto, aumentar su escala. Por fortuna, su impacto fue menor de lo esperado, ya que el apagón duró apenas una hora. Sesenta largos minutos para los habitantes de Kiev, que se quedaron sin luz.

«Cómo una nación entera se convirtió en el laboratorio de pruebas de Rusia para la guerra cibernética»: así titulaba *Wired*[10] un análisis del asunto publicado en 2017. «Los *hackers* rusos están aprendiendo a sabotear la infraestructura y Estados Unidos podría ser el siguiente.» En efecto, así fue. De modo premonitorio, *Wired* advirtió sobre lo que estaba pasando en ese mismo momento. Ese año, 2017, un grupo de *crackers* rusos denominado Dragonfly logró obtener acceso remoto a las salas de control de numerosos proveedores de energía de Estados Unidos. En 2018, cuando se

descubrió,[11] el ataque seguía aún activo. El acceso podría haberles permitido cerrar redes y causar apagones.

No fue a este grupo al que se le imputaron los ataques a la red eléctrica ucraniana, sino a otro grupo ruso de piratas informáticos, llamado Sandworm. Fue el mismo que en junio de 2017 utilizó otro programa maligno (Petya) para infectar los ordenadores de bancos, ministerios, periódicos y empresas de electricidad en Ucrania y, en menor medida, en Francia, Alemania, Italia, Polonia, Rusia, Reino Unido, Estados Unidos y Australia.

El grupo Sandworm tiene el dudoso honor de ser el autor, según la NSA, de un ataque masivo a servidores de *e-mail* activo desde agosto de 2019. La NSA advirtió en mayo de 2020 de que este grupo había estado atacando servidores de correo electrónico Exim, el sistema con el que funcionan casi la mitad de los servidores de correo electrónico de internet. Un 50 por ciento de ellos, aproximadamente, estuvieron expuestos durante más de nueve meses al ataque de Sandworm, que podría haber permitido a los *crackers* tomar el control de servidores, deshabilitar las configuraciones de seguridad de múltiples redes, añadir usuarios privilegiados o permitir accesos remotos adicionales, entre otras cosas.

Tal vez lo anterior resulte ajeno o lejano, pero podría suceder aquí mismo y afectaros a ti y a tus seres queridos. ¿En qué medida? ¿Está en riesgo el mundo, algún país o una red de ciudades de sufrir un ciberataque contra las redes eléctricas? Los expertos consultados lo creen improbable, pero reconocen la imposibilidad de saberlo. Lo que sí es cierto es que en 2021 las posibilidades no han hecho más que incrementarse, con técnicas y programas de ofensiva cibernética cada vez más avanzados. El escenario planteado por la Universidad de Cambridge para Lloyd’s señala cómo el daño en cincuenta generadores de Estados Unidos —causado por un programa malicioso como CrashOverride— podría provocar una interrupción masiva de electricidad que afectaría a noventa y tres millones de personas durante un periodo de hasta dos semanas.

Si bien este no es un escenario real, no es en absoluto irrealizable. Tirar abajo todo el sistema eléctrico de un país es una hipótesis que no se contempla, pero, como cada vez recalamos más en las redes y sistemas de información y menos en lo analógico, cada vez aumenta la posibilidad de que pueda pasar. Así lo reconoce Sánchez, del CNPIC.

De hecho, en el Informe Anual de Seguridad Nacional 2019[12] del Gobierno de España, el mayor riesgo a corto plazo, en el número uno de la lista, era la vulnerabilidad del ciberespacio. El documento alerta sobre los ciberataques a infraestructuras críticas, que pueden dañar el suministro de servicios esenciales. También pronostica que, de seguir así, en 2022 se podrían haber duplicado los ciberataques de 2019 (un total de casi cuarenta y tres mil a redes del sector público y más de ciento siete mil a empresas, ciudadanos y universidades).

> La gente pregunta a menudo: «¿Cuál será la próxima COVID?». Un ataque a nuestra infraestructura digital es uno de los principales candidatos. El coronavirus tardó varios meses en propagarse por el mundo e infectar a millones de personas. Nuestra infraestructura digital podría colapsar en un solo día.
>
> YUVAL NOAH HARARI[13]

En ese mismo informe, el Gobierno español consideraba la posibilidad de una pandemia en España como el penúltimo de su lista de quince riesgos para la seguridad nacional, seguido de la proliferación de armas de destrucción masiva. El coronavirus SARS-CoV-2 ni estaba ni se le esperaba, y sin embargo llegó. No es que no se hubiera advertido de ello: los científicos habían alertado ya en 2007 de que algo así podía suceder, de que la presencia de coronavirus en murciélagos en China era una bomba de relojería.[14]

Algunas de las reacciones y sucesos que podría desencadenar un apagón eléctrico los vivimos, de hecho, durante la pandemia que arrancó en 2020. Compras impulsivas al comienzo, reducción generalizada del consumo, cierre temporal o parcial de fronteras, quiebra y cierre definitivo o temporal de empresas y comercios, una contracción económica histórica, etc.

Eso sin contar el aumento de la brecha de desigualdad, con una pandemia que se ha cebado más con los más pobres, dependientes y vulnerables; la práctica paralización de la educación; los picos de desempleo; el efecto negativo en la salud mental de la población; la justificación de medidas totalitarias; el aumento de los ciberataques o la «pandemia» de desinformación paralela.

Todo ello sin que hubiera problemas de funcionamiento de las infraestructuras críticas y esenciales, sin problemas considerables de abastecimiento, con electricidad y luz, con agua, con movilidad (al menos para necesidades básicas) y con internet. Si esto fuera una serie de Netflix sobre lo mal que podrían ponerse las cosas ante un apagón eléctrico en comparación con la situación de la pandemia, tendrían el reclamo publicitario perfecto: «Si pensabas que el coronavirus fue catastrófico, espera a ver esto».

Peor aún: ¿y si hubiera habido un apagón de internet durante la pandemia de la COVID-19? ¿O si algo así sucediera en la próxima crisis epidémica? Su efecto no se limitaría al pequeño inconveniente de no poder ver series *online*, o de la imposibilidad de disfrutar del abanico de opciones de entretenimiento que ofrece la red, o de no poder teletrabajar, comprar *online* o ver a nuestros seres queridos de la única forma posible durante el confinamiento. Hablamos de infraestructuras críticas afectadas (porque, aunque siguiera habiendo electricidad, todo está conectado a internet), de multiplicación de los efectos económicos y en la población más vulnerable, de un caos tan absoluto que, dependiendo de la extensión geográfica y temporal de la caída, podría llevar de un estado de alarma a un estado de excepción.

Las tecnologías de la información y la comunicación (TIC) son un servicio crítico, el más esencial junto con la electricidad; son una actividad central del sistema. Todos los sectores dependen de alguna forma de ellas, en particular las finanzas, los servicios y el comercio minorista. La mayoría de los sectores dependen de las transacciones financieras electrónicas, el correo electrónico e internet para la actividad comercial. Ninguno de estos sistemas estaría operativo. Además, cuando no funcionan las comunicaciones es muy difícil para las agencias de respuesta saber qué áreas han sido afectadas y dónde priorizar los recursos, lo que ralentiza la recuperación y prolonga también el parón económico (no olvidemos que las TIC son un contribuyente significativo al valor agregado en la economía).

Hemos deconstruido todas las estructuras organizativas en la era analógica y las hemos reemplazado por una infraestructura tecnológica más eficiente, pero que nos deja expuestos. Hablamos de dependencia y salimos del coronavirus aún más dependientes —si cabe— de internet; más digitalizados y, por tanto, más vulnerables ante su derrumbe.

Ni estábamos preparados para la COVID-19 ni lo estamos para una desconexión total. Nadie invierte lo suficiente en prevenir catástrofes de este tipo hasta que algo grave pasa, entre otras cosas porque es una inversión poco rentable en términos económicos a corto plazo y también en términos políticos (como los efectos, si se ven, solo se muestran a largo plazo, dificulta atribuirse el mérito).

Lo mismo pasa con la ciberseguridad: nadie, ni empresas ni gobiernos, invierte lo suficiente en ella hasta que les estalla en las narices. El pensamiento subyacente es que sale más a cuenta ahorrar dinero cada año y asumir el riesgo.

Como dice Mary Renault en *El auriga*: «Solo hay un tipo de sobresalto peor que el totalmente inesperado: el esperado “para el cual uno se ha negado a prepararse”». En efecto, los riesgos de no hacerlo son muchos, crecientes y de mayor magnitud. Cada vez es más fácil para los ciberpiratas (que pueden ser simples usuarios con malas intenciones) causar estragos desde el sofá de su casa y sin tecnologías muy sofisticadas ni mucho conocimiento técnico. Ataques que hace unos años podían costar millones de euros hoy pueden perpetrarse cómodamente desde un portátil.

Es el lado más sombrío de internet. La Gotham City del universo *online*. En el próximo capítulo exploramos cuán oscura puede volverse.

Segunda parte

Tinieblas

3

Crimen

—El lado oscuro de la Fuerza son ellos. […] ¿Es más poderoso el lado oscuro?
—No, no. No. Más rápido, más fácil, más seductor.

La guerra de las galaxias, episodio V: *El imperio contraataca*

En el ciberespacio, la ofensiva tiene la ventaja.

William J. Lynn III, ex subsecretario de Defensa de Estados Unidos

Hasta un niño podría hacerlo. Literalmente. Un ciberataque épico contra Twitter, el mayor de todos los tiempos, lo cometió un menor de edad el 15 de julio de 2020. El estadounidense Graham Ivan Clark logró hacerse con el control de las cuentas de ciento treinta personas en la red social. En concreto, de celebridades o de figuras reconocidas, como Barack Obama, Joe Biden, Bill Gates, Elon Musk, Kanye West o Kim Kardashian. A cambio, recibió ciento veintiún mil dólares procedentes de más de cuatrocientos pagos a tres direcciones Bitcoin diferentes.

Clark no lo hizo solo. Al cerebro de la operación le ayudaron al menos otras tres personas. Entre ellas, el británico Joseph O’Connor, detenido en Estepona en julio de 2021. Los otros tres habían sido arrestados un año antes, tan solo dos semanas después del ciberataque. Su juventud causó sorpresa, a pesar de que no es nuevo para la policía encontrarse con jóvenes ciberpiratas extremadamente sofisticados. Adolescentes que, como Clark, han pasado su infancia sumergidos en las profundidades de internet, buceando en sus tinieblas.

Muchos de esos menores, como Clark, son jugadores de Minecraft, el videojuego más vendido de la historia. Según sus seguidores, Minecraft es altamente adictivo. Lo que en un principio engancha son sus infinitas posibilidades de construcción y exploración de mundos, la perfecta fantasía infantil. Sin embargo, los jugadores no se quedan por eso; o no solo por eso. Lo que ofrece Minecraft, además de un espacio de juego, es una comunidad, un lugar donde encontrar a sus mejores amigos. Esta combinación ideal ofrece una realidad alternativa a los usuarios, que a menudo se refugian en el videojuego como vía de escape a los problemas familiares, a una dura infancia o a una adolescencia infeliz.

A veces, el juego traspasa las fronteras de lo virtual a lo real. Un grupo de estudiantes enganchados al juego protagonizó la historia de ciberpirateo más sonada de 2016. Lo hicieron a través de la creación de Mirai: una inédita *botnet*. Una *botnet*

es una gran red de ordenadores conectados y coordinados para realizar una tarea. En este caso, una con malas intenciones que acabó afectando a servicios clave de internet en todo el mundo. Es el ejemplo clásico de cómo usar una buena tecnología para hacer el mal.

La estrategia usada fue un ataque de denegación de servicio distribuido (DDoS) **[*]**. El objetivo de estos ataques es degradar tanto la calidad del servicio de un sistema que este quede inhabilitado. Una de las empresas atacadas fue DynDNS, un pilar clave de la red de redes. ¿Recuerdan que en el capítulo 1 hablábamos de cómo internet podría caer a través de un ataque a los DNS, a los nombres de internet? ¡Equilicuá! El asalto supuso la práctica paralización de internet en casi todo el este de Estados Unidos. Fue la mayor ofensiva de ese tipo realizada hasta el momento.

Los estudiantes que orquestaron tal asalto no tenían, al parecer, la intención de derribar internet. Simplemente trataban de obtener puntos extra en Minecraft perpetrando ataques DDoS contra sus rivales. «No se dieron cuenta del poder que estaban desatando», dijo un agente del FBI que había investigado el caso en su momento.**[1]** Como el proyecto Manhattan, que resultó en la creación de la bomba atómica, comenzó como un reto y se les acabó yendo de las manos (salvando las distancias, claro está).

El peligro de las *botnets* se popularizó gracias a otro joven, un canadiense conocido como MafiaBoy. En el año 2000, este quinceañero llamado Michael Calce atacó sitios web como Amazon, CNN, Dell, eBay o Yahoo (que, por aquel entonces, era el mayor motor de búsqueda del mundo). La estrategia: sobrecargar sus redes para hacerlas colapsar. Fue uno de los primeros ataques DDoS registrados. La travesura puso de manifiesto la amenaza que este tipo de ofensiva supone para la integridad y estabilidad de internet. Incluso sin intención, incluso viniendo de unos niños.

Como dice el criptógrafo Bruce Schneier, en el mundo *online* el ataque es más fácil que la defensa.**[2]** La complejidad de los sistemas informatizados se traduce en una menor seguridad: más personas e interacciones implicadas, más errores en el proceso de diseño y desarrollo. Los atacantes tienen la ventaja del primer movimiento, no suelen preocuparse por las leyes o la ética convencionales, y normalmente tienen más recursos para acceder a las tecnologías más punteras. Eso, junto con la difícil atribución de los delitos *online* y la persecución de los ciberdelincuentes, añadido a los problemas jurisdiccionales que acarrea el carácter internacional de la red de redes.

Hemos pasado de vivir en un mundo intrínsecamente seguro a uno intrínsecamente inseguro.**[3]** Tuvieron que transcurrir cientos de años entre la invención de la armadura y la creación, mucho después, de la ballesta capaz de penetrarla. Ahora, entre las medidas y contramedidas de seguridad, se tardan minutos o días o, como mucho, escasas semanas. No es posible contar con una garantía de protección absoluta, y los ataques no cesan. Uno de los estudios más citados sobre la frecuencia de los delitos *online* dice que hay un ciberataque cada treinta y nueve

segundos. El estudio es de 2007. Imagínense cuántos ataques por minuto hay hoy, más de catorce años después y con todo un nuevo arsenal de herramientas disponibles para multiplicar el cibercrimen.

Las posibilidades de crimen o delito *online* se multiplican también debido a la hiperconectividad. Ya lo decíamos antes: prácticamente todo está conectado a internet, y lo que aún no lo está va camino de estarlo. Los frigoríficos analógicos, las cafeteras o cualquier tipo de electrodoméstico corren el peligro de quedar desfasados por no estar *online*. Que tenga sentido o no, no parece importar mucho. Estamos en la era de los objetos inteligentes: móviles, altavoces, zapatillas, relojes, camisetas, pulseras, anillos, juguetitos sexuales y hasta peceras. ¡Peceras! De hecho, una pecera conectada a internet permitió a un ciberdelincuente de Finlandia robar datos del casino donde estaba instalada.[4]

Esa anécdota, que sucedió en 2016 en Estados Unidos, ilustra cómo en el IoT (Internet of Things), el internet de los objetos conectados, hasta los más anodinos y supuestamente tontos aparatos pueden servir como puerta de entrada a ciberdelincuentes que podrían causar importantes daños. Ya hay, y habrá cada vez más, objetos de todo tipo conectados a internet, casi hasta donde alcance la imaginación. Hace poco más de una década, una radio o un camión no eran susceptibles de sufrir un ataque informático. Ahora sí, porque todo se está convirtiendo en un ordenador: objetos (dinero incluido), infraestructuras, fábricas… También las personas nos hemos vuelto entes conectados, a través de marcapasos y otros implantes, bombas de insulina o incluso microchips que los autodenominados «cíborgs» se implantan voluntariamente. El genio y figura de Elon Musk (entre muchos otros) quiere conectar hasta nuestro cerebro.

A la internet a palo seco se suman la internet de las cosas y la internet de los humanos; una internet aumentada en el que incluso las cosas que no interactúan directamente se influyen las unas a las otras. Las interconexiones dificultan entender qué sistema está fallando. Incluso puede ser que ninguno funcione mal y que la causa sea una interacción insegura de dos sistemas que, por separado, son seguros. Cien sistemas que interactúan entre sí suponen cinco mil interacciones y, por tanto, cinco mil puntos débiles. Si mil sistemas interactúan, hablamos de medio millón de interacciones. Y así sucesivamente.

La creciente conectividad de todas las cosas y sus interacciones tienen otra consecuencia: el campo que hoy denominamos «seguridad informática» acabará siendo —como dice Schneier— la seguridad de todo. Esto abre dos posibilidades. Una: que todo pueda usarse contra nosotros. Dos: que pueda atacarse la infraestructura crítica global. Ambas pueden conducir a escenarios aterradores, como ya hemos visto.

EL TOP 10 DEL CIBERCRIMEN

En páginas anteriores señalábamos algunos ataques DDoS mediante *botnets*. Si bien este es un tipo de ofensiva con un potencial alto de impacto, no es el único. Y ejemplos no faltan. Los hay para todos los gustos:

Gusanos

Hablábamos en el capítulo 2 de Industroyer como la mayor amenaza para los sistemas de control industrial desde Stuxnet. Este último es un gusano informático que en 2010 eliminó alrededor de una quinta parte de las centrifugadoras nucleares de Irán. También contribuyó a retrasar su capacidad para fabricar armas nucleares. Sus autores pudieron espiar los sistemas industriales e incluso hacer que se autodestruyeran sin el conocimiento de los operadores humanos. Todo esto lo sabemos ahora, pero durante varios meses la causa fue un absoluto misterio.

Un gusano es un sistema malicioso que se propaga de ordenador a ordenador por sí solo, sin mediación humana. Stuxnet no se parecía a ningún otro virus o gusano anterior; era un código malicioso y magistral sin precedentes. En lugar de limitarse a secuestrar determinados ordenadores o a robar información, pasó del ámbito digital a destruir físicamente los equipos controlados por dichos ordenadores.**[5]** De hecho, estos no estaban conectados a internet. Por eso, los atacantes diseñaron un arma capaz de propagarse a través de memorias USB infectadas.

Hablando de gusanos: entre los primeros desastres de seguridad del presente siglo está el gusano ILoveYou. Se difundió en el año 2000 y tenía como gancho un correo electrónico con el asunto «Te quiero». Un archivo adjunto con una supuesta carta de amor era lo que, al abrirse, activaba el virus. Su código malicioso infectó nada menos que al 10 por ciento de todos los ordenadores del mundo. Más de cuarenta y cinco millones de máquinas en veinticuatro horas.

El Pentágono, la CIA y el Parlamento del Reino Unido cerraron sus sistemas de correo electrónico en respuesta al incidente y muchas otras organizaciones desconectaron parte de su infraestructura. Las estimaciones de los costes económicos asociados rondan los diez mil millones de dólares. Por cierto, su autoría acaba de ser confirmada. Se sospechaba que el ataque había sido obra de un filipino llamado Onel de Guzmán, algo que él mismo reconoció en mayo de 2020,**[6]** veinte años después. A sus cuarenta y cuatro años, De Guzmán admitió que lo hizo para robar contraseñas y poder acceder a internet sin pagar. También dijo que su intención no era que el gusano se extendiera a escala mundial y que lamentaba el daño que su código había causado.

Secuestradores

En el bosque, Robin Hood robaba a los ricos para dárselo a los pobres. En el ciberespacio, RobbinHood secuestra información para robar a empresas y gobiernos. O, más bien, para extorsionarlos. Tiene forma de *ransomware*, un tipo de programa malicioso que impide usar el equipo o equipos afectados, o acceder a ciertos archivos, hasta que se pague un rescate.

En 2019, RobbinHood echó abajo gran parte de los servicios de la ciudad de Baltimore (Estados Unidos) mediante un ataque a los servidores municipales. Correos electrónicos caídos, líneas de teléfono afectadas, imposibilidad de pagar telemáticamente los tributos…; muchas actividades que se solían realizar *online* tuvieron que llevarse a cabo en persona. Se cerraron prácticamente todos los sistemas que no eran de emergencia. Las largas colas en el ayuntamiento y el completo desorden administrativo provocado duraron más de un mes.

¿Les suena de algo? Algo muy parecido le sucedió en España al SEPE, el Servicio Público de Empleo Estatal, en marzo de 2021. El atacante no fue RobbinHood, sino Ryuk, un siniestro personaje de la serie manga *Death Note*. Es el nombre del *ransomware* que dejó noqueado durante más de dos semanas al organismo que, entre otras cosas, gestiona las prestaciones por desempleo. En un momento, el SEPE retrocedió veinte años en la atención al público. No era posible realizar ningún trámite (ni *online* ni presencialmente) y tuvieron que recurrir a rellenar a mano antiguos formularios en papel.[7] Los atacantes procedían de Rusia y, según el SEPE, no pidieron un rescate por volver a la normalidad,[8] algo bastante inusual.

En el caso de Baltimore, los secuestradores sí pidieron algo a cambio del desbloqueo de los servicios: trece bitcoins (algo menos de cien mil dólares). El alcalde no pagó, pero sí el regidor de Lafayette, otra ciudad estadounidense que en julio de 2020 sufrió un ataque similar. El motivo que adujo para hacerlo fue que el coste-beneficio del rescate superaba «con creces» la opción de reconstrucción posterior.

Estos son solo algunos de los numerosos ejemplos de secuestros de datos mediante *ransomware*, que en 2020 causaron pérdidas económicas por valor de cientos de miles de millones de dólares.[9] En el caso de España, se registraron 8.475 ataques con un coste estimado de cerca de 1.200 millones de dólares. Muchos de esos ciberasaltos afectaron a administraciones públicas (gobiernos locales y regionales) y también a varios ministerios y universidades, o a entidades como el Banco de España.

El uso de estos programas maliciosos crece de forma exponencial. Cada vez son más fáciles de ejecutar y más lucrativos para los delincuentes. Estos juegan con varias ventajas: un creciente volumen de dispositivos conectados y, por tanto, secuestrables; avances de la criptografía que facilitan el secuestro, y sistemas de pago anónimo internacionales que dificultan rastrear el delito y facilitan que los piratas puedan lanzar ataques masivos mientras su identidad permanece oculta.

Un ejemplo claro de los estragos que pueden llegar a causar este tipo de atacantes es WannaCry. A su lado, Ryak o RobbinHood son una pura anécdota. No hablamos del SEPE o de una pequeña ciudad estadounidense afectada, sino de más de 150 países, más de 360.000 dispositivos electrónicos bloqueados y más de 200.000 víctimas.[10] En solo unos pocos días, causó unas pérdidas de miles de millones de dólares.

El ataque se produjo entre el 12 y el 16 de mayo de 2017. Su potencia y alcance mundial se explican en gran medida por su capacidad de actuar como gusano y propagarse automáticamente sin necesidad de interacción humana. Además, aprovechaba un fallo de seguridad de Windows que afectaba a millones de personas. España fue uno de los primeros países perjudicados (Telefónica decidió apagar todos sus equipos). No fue, sin embargo, una de las mayores víctimas deWannaCry. Mucho peor parado salió el National Health Service (NHS) del Reino Unido, con más de seiscientas organizaciones afectadas.[11]

Un mes después de este ciberataque, otro de características similares —llamado NotPetya— afectó a varios países. Y ¡sorpresa!, utilizaba la misma vulnerabilidad de Windows para infectar los ordenadores. Una vulnerabilidad a la que, por cierto, seguían expuestos 1,7 millones de terminales en 2019.[12] Aun después de haber sufrido las consecuencias de estas ciberofensivas y a pesar de existir una solución contra los fallos de seguridad expuestos, la negligencia y falta de prevención siguen minando la ciberseguridad mundial.

Suplantadores

En agosto de 2020, varios ministros del Gobierno español sufrieron un ciberataque a través de sus teléfonos móviles. El vehículo fue la aplicación de mensajería instantánea Telegram, donde los afectados recibieron un mensaje que procedía supuestamente de una importante embajada en España y que pedía hacer clic en un enlace para más información. Al hacerlo, el contenido de sus teléfonos quedaba expuesto a los atacantes.

Se trata de un ejemplo clásico de *phishing* o suplantación de identidad: una táctica de ciberataque en la que los delincuentes se hacen pasar por personas u organizaciones legítimas para obtener datos personales o información sobre sus cuentas bancarias, contraseñas, etcétera.

El *phishing* es el tipo de ataque informático más común. La lista de organizaciones que son suplantadas con frecuencia es larga: bancos, sistemas de pago, redes sociales, páginas de compraventa, servicios de mensajería, juegos *online*, cuerpos policiales, instituciones públicas… Los piratas utilizan pretextos de todo tipo: problemas técnicos, cambios en la política de seguridad, detecciones de fraude, accesos anómalos a tu cuenta, la inminente desactivación del servicio, falsas ofertas de empleo, premios, regalos, ingresos económicos inesperados…

> ¡Felicitaciones! ¡Hoy está de suerte! Es usted uno de los diez usuarios seleccionados para recibir al azar el nuevo iPhone 12. Para recibir su regalo, solo tiene que hacer clic en el siguiente enlace.
> Estimado cliente: su usuario se ha desactivado temporalmente por razones de seguridad. Por favor, confirme su identidad actual haciendo clic aquí o la cuenta se desactivará.

Son tan solo algunos ejemplos. Cada día, cientos de millones de organizaciones y personas sufren alguna forma de *phishing*. Solo Google bloquea a diario cien millones de ataques de *phishing* contra usuarios de Gmail.[13] Pero estos ataques se dan también a través de mensajes SMS, aplicaciones, redes sociales, falsos sitios web… Es, de hecho, el tipo de delito más común en internet. Solo en Estados Unidos, más de 114.000 víctimas perdieron casi 58 millones de dólares[14] como resultado de una estafa de este tipo en 2019.

A veces, los ciberdelincuentes se equivocan y propician nuevos ataques, como cuando dejaron al descubierto miles de contraseñas robadas al suplantar la identidad de la empresa Xerox y permitieron que cualquier persona pudiera encontrarlas con una simple búsqueda en Google.[15] Algo por el estilo sucedió cuando un *hacker* filtró los números de teléfono y los datos personales de quinientos usuarios de Facebook, lo que comprometió la seguridad de sus cuentas y su privacidad.[16]

Cada maestrillo tiene su librillo y algunos cibercriminales usan técnicas más sofisticadas que otros. Un tipo de suplantación llamada *spoofing* consiste en duplicar la dirección o el teléfono de alguien (incluso la localización GPS). Es lo que le sucedió a una serie de buques de guerra estadounidenses que colisionaron en 2017 en varias localizaciones. Al menos cuatro accidentes de barcos de la Séptima Flota de la armada de Estados Unidos en menos de un año. Los investigadores encontraron un problema común: los barcos pensaban que se encontraban en una ubicación diferente de la real. Fueron víctima de piratas, pero no de los que surcan los mares, sino de los que navegan en internet. Concretamente, se cree que fue un experimento de *crackers* rusos que aprovecharon la alta dependencia de la navegación marítima en las redes informáticas.

Cazaballenas

En 2016, un grupo de ciberdelincuentes chinos pasó una temporada escondido en las redes informáticas de Mattel (la multinacional que fabrica la muñeca Barbie o los juguetes para bebés Fisher-Price). Antes de pasar a la acción, estos estafadores debían estudiar los procedimientos internos de la corporación, los protocolos, la jerarquía corporativa, la información de los proveedores, las personalidades de los empleados, etc. Todo formaba parte de su plan de cazaballenas. El momento perfecto para lanzar su ataque llegó cuando Mattel decidió nombrar a un nuevo director general, Christopher Sinclair.

Los atacantes usaron la identidad de Sinclair para enviar un correo electrónico en su nombre. En él, solicitaban al destinatario una aprobación conjunta del abono a un proveedor chino de Mattel. El pago de tres millones de dólares debía transferirse a un banco de Wenzhou (China). Según el protocolo interno de Mattel, dicho pago requeriría la autorización de dos gerentes de alto nivel. Como la solicitud provenía (supuestamente) del nuevo mandamás, dichas personas dieron el visto bueno. Cuando los directivos se percataron, la transferencia ya se había ordenado. Por fortuna para Mattel, ese día era un festivo bancario, lo que le dio tiempo —con la cooperación de las autoridades chinas— para recuperar el dinero antes de ser transferido.

Esta historia, de forma excepcional, tuvo un final feliz. El suceso refleja, tal cual, la esencia de un ataque «de cazaballenas». Su nombre alude al tamaño del animal: si algo tienen las ballenas es que son grandes, tanto como la ambición de los atacantes. Un ataque de cazaballenas es, en realidad, un ataque de *phishing* dirigido a un tipo de objetivo muy específico (no aleatorio, como en el *phishing* tradicional), al que se estudia con anterioridad (como hicieron los chinos con Mattel), con intención enfáticamente maliciosa y con una potencial ganancia mayor.

Los cazaballenas se fijan frecuentemente en altos ejecutivos. El propósito es hacerse pasar por ellos con la esperanza de aprovechar su autoridad para obtener acceso a datos confidenciales o para motivar conductas en su favor (como lo era la transferencia bancaria de tres millones de dólares de Mattel). ¿Cómo? Ya lo hemos visto: mediante *e-mails* a sus empleados en los que se hacen pasar por esas personas para pedir lo que desean.

Ciberespías

En diciembre de 2020 se descubrió el mayor ciberataque hasta la fecha en Estados Unidos. Una obra de ciberespionaje criminal en toda regla que permitió a los atacantes husmear en las entrañas de varios ministerios (entre ellos los departamentos de Defensa, Seguridad Nacional y del Tesoro). También se colaron en otros muchos organismos oficiales y en grandes empresas como Microsoft. Pudieron hacerlo a través de un *software* común a todas ellas, que les permitió acceder a las tripas del sistema. El *software* pertenecía a la empresa SolarWinds. ¿Adivinan cuál era su contraseña? Sí, han acertado: «Solarwinds123».[17]

Otra historia de ciberespías se saldó con el misterioso asesinato, el 2 de octubre de 2018, del periodista saudí y columnista del diario *The Washington Post* Jamal Khashoggi. Su prometida le vio por última vez entrando en el consulado de Arabia Saudí en Estambul, al que fue a solicitar un certificado de divorcio para poder casarse con ella. Desde entonces no se le volvió a ver vivo. Un informe[18] de las agencias de inteligencia de Estados Unidos hecho público por el presidente Joe Biden apuntaba al príncipe heredero Mohamed bin Salmán como responsable del asesinato, a quien con anterioridad fuentes de la ONU habían señalado también.

La historia de Khashoggi no figuraría en este libro de no ser por un pequeño detalle: el columnista fue identificado como víctima del *software* espía Pegasus; un programa que, no por casualidad, fue usado para espiar al mismo tiempo a dos personas cercanas a Khashoggi y al propio Jeff Bezos, propietario de *The Washington Post*. Su forma de hacerlo es mediante enlaces maliciosos en mensajes de texto o brechas de seguridad en *apps* (por ejemplo, en WhatsApp) para hacerse con el control de los dispositivos móviles. De este modo, los espías pueden conocer qué teclas pulsa el usuario en todo momento, tomar el control de la cámara y el micrófono del teléfono o acceder a su ubicación, a listas de contactos, a sus archivos o a mensajes cifrados.

Así es como Pegasus, propiedad de la empresa israelí NSO Group, espió también al presidente del Parlament de Cataluña, Roger Torrent, y al diputado autonómico catalán Ernest Maragall. El programa solo pueden adquirirlo los servicios de inteligencia estatales y las fuerzas de seguridad —se supone que para prevenir e investigar actos de terrorismo y crímenes—, y casualmente los servicios secretos españoles figuran en la lista de clientes de NSO Group.[19]

Controladores

Pongámonos en situación. Vamos por la carretera conduciendo nuestro coche a ciento veinte kilómetros por hora y, de pronto, este se cambia de carril, se activan los limpiaparabrisas, empieza a sonar música a todo volumen, se bloquean las puertas y se desactivan los frenos sin que podamos hacer nada por evitarlo. La pérdida del control del vehículo es total. Un escenario que podríamos encontrar en nuestras peores pesadillas o… en la realidad.

El milagro es, de hecho, que no haya pasado ya. Los automóviles, como cualquier otro dispositivo conectado, son susceptibles de ser pirateados. Y las consecuencias en ese caso pueden ser fatales. Lo demostraron en 2015 un par de *hackers* que lograron tomar el control de un Jeep Cherokee 2014 desde su casa, a más de quince kilómetros de distancia de donde se encontraba el vehículo. El coche en cuestión lo conducía Andy Greenberg, periodista de la revista *Wired*. La hazaña fue grabada y transmitida en YouTube.[20] Como resultado, Fiat Chrysler llamó a la retirada del mercado de casi un millón y medio de estos vehículos para actualizar su *software* y evitar así el posible ataque.

La pregunta es: si esto puede pasar con un coche o con cualquier tipo de dispositivo o vehículo, ¿por qué no con un avión? En efecto, también ha sucedido. En 2017 un equipo de *hackers* del Departamento de Seguridad Nacional (DHS) de Estados Unidos logró piratear y controlar de forma remota un avión Boeing 757 estacionado en un aeropuerto de Atlantic City. Estos explotaron una vulnerabilidad en las comunicaciones por radiofrecuencia que los expertos en aviación dicen conocer desde hace años. ¿Por qué, entonces, nadie lo ha arreglado? Por lamentable que

parezca, la razón es obvia: cuesta demasiado dinero y tiempo, alrededor de un millón de dólares por cada aparato en un plazo de un año; algo que para aerolíneas pequeñas podría suponer la bancarrota. Eso sin mencionar que el DHS calculaba entonces que un 90 por ciento de los aviones comerciales podrían estar afectados por esa vulnerabilidad.

Rompelotodos

¿Alguna vez se ha preguntado cuán seguras son las llaves electrónicas en forma de tarjeta que dan en los hoteles? Por lo general, tendemos a confiar en que son un buen sistema y en que todo estará en su sitio cuando regresemos a nuestra habitación. Es lo que debió de pensar la consultora de tecnología Janet Wolf cuando salió de su cuarto en uno de los hoteles Hyatt de Houston (Estados Unidos) para dirigirse a una reunión de negocios. Cuando regresó, todo estaba en orden, excepto por una cosa: su ordenador portátil había desaparecido.

Tras el misterio inicial, se descubrió que las cerraduras de todas las habitaciones del hotel habían sido pirateadas. Los atacantes habían aprovechado un problema de seguridad de Onity, la compañía cuyas cerraduras protegen más de cuatro millones de habitaciones de hotel en todo el mundo, en instalaciones de Hyatt, Marriot, InterContinental, Meliá, Husa o NH Hoteles. (Por cierto, la presencia de tantas firmas españolas no es casual, ya que la actual Onity, creada hace más de veinte años, no es otra que la antigua compañía vasca Talleres de Escoriaza [TESA Entry Systems], nacida en 1941.)

El caso es que la vulnerabilidad había sido ya denunciada por expertos en ciberseguridad meses atrás. Cualquier *cracker* podría construir, por menos de cincuenta euros, un dispositivo casero capaz de abrir en cuestión de segundos las habitaciones con la tecnología de Onity. Más de nueve meses después de que la empresa anunciara una solución para este fallo, los ladrones siguieron sirviéndose de él para robar por doquier sin apenas dejar rastro.

Este tipo de ataque se conoce como «rotura de clase» porque afecta no solo a un sistema, sino a toda una clase de sistemas. Una vez que alguien descubre un fallo de seguridad, puede automatizar el ataque a través de internet y transmitir esa habilidad a otras muchas personas. Como constata Schneier, a medida que nos adentramos en el mundo de la internet de las cosas, las roturas de clase serán cada vez más frecuentes. También con un potencial impacto mayor, ya que la combinación de automatización y acción a distancia dará a los atacantes más poder.

Troyanos

Cuenta la conocida leyenda de la guerra de Troya que los griegos se escondieron dentro de un supuesto regalo en forma de caballo de madera gigante para acceder a la ciudad teucra y tomarla desde dentro. Del mismo modo, el *software* malicioso troyano se infiltra en su sistema disfrazado como una herramienta legítima y, una vez dentro, comienza a atacar. Dependiendo de sus capacidades, podrá acceder y capturar desde inicios de sesión y contraseñas hasta pulsaciones de teclas y detalles bancarios, tomar capturas de pantalla o incluso modificar datos.

Uno de los casos más conocidos de caballos de Troya *online* es Emotet, calificado por el Departamento de Seguridad Nacional (DHS) de Estados Unidos como «uno de los programas maliciosos más caros y destructivos». Se trata de un troyano bancario que empezó difundiéndose a través de correos electrónicos de entidades financieras que contenían archivos adjuntos o enlaces perniciosos. Ahora su uso ha evolucionado hasta convertirse en distribuidor de otros programas o campañas malignos.

Se estima que el coste de recuperación de este tipo de ataque supera el millón de dólares por evento. Emotet es uno de los troyanos *online* más buscados, dado que, además, destaca por utilizar múltiples métodos y técnicas de evasión para evitar ser detectado. En España ha llegado a liderar los rankings como el país más perjudicado por este troyano, con más de un 17 por ciento de compañías afectadas en agosto de 2020, casi cuatro puntos más que la media global de ese mes.[21]

Cibercupidos

Te buscan, te investigan, te camelan, te prometen la luna y, cuando estás de amor hasta las trancas, te piden dinero. No es un ciberataque como tal, sino una forma de timo, pero una muy común. Los ciberdelincuentes del amor se aprovechan de que cada vez más personas buscan amor, sexo, amistad o simplemente compañía en diferentes webs, redes sociales y aplicaciones móviles. Su propósito final es obvio: conseguir efectivo.

Los profesionales del embaucamiento *online* crean perfiles falsos para convencer a los usuarios de que les envíen dinero. Para ello aprovechan perfiles abiertos de otras personas en redes sociales, generalmente de buen ver y en buena forma. De ellos obtienen fotos, nombres y otros datos con los que montar una historia convincente. Luego seleccionan a sus víctimas, a veces con cierta investigación previa para conocer de antemano al objetivo que se va a engatusar. Aprovechan también perfiles abiertos que ofrecen información suficiente como para adaptar sus mensajes.

Una vez que el usuario o usuaria en cuestión ha caído en sus brazos, los engatusadores buscan cualquier excusa para justificar una transferencia bancaria. Por ejemplo, que necesitan dinero para viajar a verlos. También es común que simulen secuestros para pedir rescates, o que usen imágenes íntimas de la víctima para extorsionarlas. Esto último se conoce como «sextorsión», que es básicamente una forma de chantaje sexual. Sus consecuencias pueden ser fatídicas, como demostró en

2019 el suicidio de una (entonces) empleada de Iveco cuando se difundió entre los compañeros de su empresa un vídeo sexual en el que aparecía con un examante.

Pedófilos y encubridores

Hacer dinero con vídeos de violaciones de niños. Es tan atroz que duele escribirlo. Por eso el escándalo fue mayúsculo cuando el dos veces premio Pulitzer y columnista de *The New York Times* Nicholas Kristof puso negro sobre blanco que eso era exactamente lo que hacía el gigante web del porno Pornhub.[22] Cientos de miles de vídeos de menores manteniendo relaciones sexuales o en situaciones vejatorias o de violencia sexual estaban disponibles en la plataforma. La polémica hizo que la empresa eliminase millones de vídeos subidos por usuarios y anunciase que solo los usuarios verificados podrían cargar nuevos vídeos en la web.[23]

El caso de Pornhub es solo la punta del iceberg. Internet es un paraíso para pedófilos y pervertidos de todo el mundo que buscan y comercian *online* con imágenes de menores de edad y que aprovechan la poca precaución de los pequeños o de sus familiares y amigos al compartir todo tipo de imágenes *online* de forma pública. Quienes van un paso más allá son los pederastas, que usan las redes como medio para encontrar a sus víctimas y pasar a la acción (al abuso sexual). Y luego lo suben a internet —o no— y aparecen en sitios como Pornhub.

En un punto intermedio, con independencia de que llegue a consumarse o no un abuso sexual físico, están los que practican el *grooming*. Estos se encubren o se camuflan bajo la apariencia de un menor de edad para establecer una relación *online* con otro menor, a quien engañan o presionan con fines sexuales: desde mantener conversaciones eróticas hasta conseguir imágenes o vídeos con una alta carga sexual. No practican la «sextorsión» a cambio de dinero, sino de más imágenes o de ceder a sus peticiones. Tan abominable como suena.

CONTRA LOS MÁS VULNERABLES

Hemos visto tan solo una ínfima parte de los millones de ejemplos de ciberdelitos que pueden ser enumerados y una gran variedad de formas en las que pueden darse. Todo ello en situaciones normales. Pero 2020 no fue un año normal. La COVID-19 llegó para cambiarlo todo. En el caso de la ciberdelincuencia, para multiplicarla. Solo en ataques de secuestro malicioso o *ransomware* hubo en España un incremento del 160 por ciento de casos.[24] Aumentaron también —un 23 por ciento— las brechas de seguridad, debido al teletrabajo y a la mayor movilidad de datos.[25] A escala global, se calcula que hubo un 25 por ciento más de ciberataques.[26]

Los malos de la red no solo explotan fallos técnicos del sistema, sino también humanos, y una pandemia proporciona el contexto perfecto para combinar ambos y hacer mucho daño. Es un cóctel explosivo por múltiples razones y con múltiples

fuentes de alimentación: teletrabajo (desde redes domésticas inseguras, a veces desde ordenadores personales), videollamadas, aumento del tiempo en internet y en redes sociales, incertidumbre en torno a la enfermedad, mayor dependencia de los servicios *online*, colapso de servicios esenciales e infraestructuras críticas más susceptibles de ser atacadas… Incluso el aburrimiento y el mayor tiempo libre de los piratas informáticos durante la cuarentena se sumaron como factores de incremento de los delitos cibernéticos.[27]

De nuevo, los ejemplos son muy numerosos. Gusanos, secuestradores, suplantadores, ciberespías y ataques de todo tipo. Vimos la primera muerte vinculada a *ransomware* tras un ciberataque al hospital universitario de Düsseldorf y cómo el hospital Moisès Broggi, en la provincia de Barcelona, se quedó sin servicio telefónico, sin correo corporativo y sin acceso a las radiografías tras una ofensiva de *crackers* rusos. Vimos el aumento del espionaje industrial y de centros de investigación cuando ciberdelincuentes chinos y rusos robaron datos de las vacunas contra la COVID-19 (incluida la española). Vimos cómo se ciberatacaba a la Agencia Europea del Medicamento (EMA, por sus siglas en inglés) y a la cadena de suministro de las primeras vacunas producidas a gran escala. Vimos en España secuestros de datos de empresas eléctricas como Endesa o EDP o de aseguradoras como SegurCaixa Adeslas. Vimos cómo aumentaba un 400 por ciento la oferta de vacunas falsas por parte de los cibercriminales que se esconden en la llamada *dark web* (una parte oculta de internet que no se puede encontrar mediante buscadores y a la que normalmente se accede mediante determinados programas).

Vimos las brechas de seguridad de Zoom de reuniones virtuales que desembocaron en la filtración de las direcciones de correo electrónico y fotos de miles de usuarios, o intentos de iniciar llamadas por parte de extraños, o extraños que se colaban en videollamadas privadas. Vimos cómo se multiplicaban los ataques de suplantación de identidad, con aumentos de más de un 850 por ciento en los casos de *phishing* por URL relacionados con Netflix.

Vimos la proliferación de *e-mails* maliciosos con supuesta información sobre la COVID-19, así como programas espía que se ocultaban bajo falsas aplicaciones contra la enfermedad. Vimos el robo de datos a múltiples organizaciones protagonizados por un joven *cracker* de dieciséis años. Vimos cómo otro adolescente de esa misma edad pirateó el sistema de aprendizaje *online* de las escuelas públicas del condado de Miami-Dade, el cuarto distrito escolar más grande de Estados Unidos. Vimos también intentos de ataque a varios aeropuertos. Eso solo por citar algunos ejemplos.

Si la COVID-19 hizo más vulnerables a los ciberataques al común de los mortales, más aún a las familias en riesgo y a los más pequeños, que aumentaron su tiempo *online* sin supervisión. Los menores están igual de expuestos que los mayores, pero por lo general cuentan con menos herramientas para hacer frente a abusadores o a estafadores. Su falta de experiencia y su ingenuidad les hacen especialmente

vulnerables. Ellos, en particular los más pequeños, no saben, no piensan o no entienden que, detrás de un ordenador, puede haber alguien que quiere beneficiarse de ellos. No perciben el riesgo como lo haría un adulto.

Además de pederastas y acosadores camuflados, los menores son víctimas frecuentes de «sextorsión», de control, acoso o abuso por iguales (ya sea escolar, sexual o de otro tipo), de timos por vía directa o indirecta para estafar a sus padres, de chantajes e intromisiones en su intimidad, etc. Muchos de estos casos no se llegan a conocer, bien porque no se difunden o bien porque no se denuncian.

Los expertos advierten: «Desconfía de cualquier estadística que veas con menores».[28] También lamentan que no hay suficientes medios técnicos y humanos para investigar todos los incidentes que se reportan. ¿Qué se ha hecho al respecto, cuántos malos se han cogido, cuántas bandas se han desarticulado? Muy pocas. Hace falta mucho dinero y no compensa. No hay presión ni alarma social. Nos da miedo que nos saquen una navaja por la calle para robarnos, pero no hay sensación de miedo a ser atracados en internet.

DE MAL EN PEOR

Esto nos lleva de vuelta al comienzo. En internet, el ataque es más fácil que la defensa. Las consecuencias ya las hemos visto: niños y adolescentes que se convierten fácilmente en ciberdelincuentes, múltiples formas de ataque al alcance de muchos, fallos de seguridad conocidos que permanecen sin solucionarse, incluso tras haberse usado para perpetrar un ataque, y malhechores *online* que se aprovechan de los más indefensos y de coyunturas excepcionales como la de una pandemia.

Todo esto no es, ni por asomo, lo peor que podría pasar. Frente a unas infraestructuras anticuadas que hacen peligrar hasta las elecciones de Estados Unidos con sistemas de recuento pirateados,[29] las técnicas de ciberataque son cada vez más sofisticadas, pero también más sencillas y baratas. Por otra parte, aparecen nuevas tecnologías que facilitan la creciente automatización de los ataques, además de multiplicar su escala. La inteligencia artificial, unida a una cada vez mayor potencia de las redes que mueven el tráfico *online*, es una bomba de relojería. En 2019, la red de la conferencia de supercomputación SC19 SCinet alcanzó una velocidad de más de cuatro *terabytes* por segundo. Es decir, un ancho de banda suficiente como para descargar en cuarenta y cinco segundos el catálogo completo de películas de Netflix. Como reconoce su guardiana, la directora de Seguridad de Redes de SCinet, Soledad Antelada, una red de este tipo en las manos equivocadas se convertiría en una autopista de ataque: ya no se necesitaría infectar a miles de ordenadores para generar el tráfico suficiente como para colapsar un sistema.

Las criptomonedas también podrían empeorar las cosas en materia de ciberseguridad. Los medios de pago digital como Bitcoin y otras criptodivisas que usan el cifrado criptográfico ofrecen a los usuarios una forma segura y fiable de

transferir dinero. Además, es posible hacerlo de manera anónima, y esto es clave; las criptomonedas son perfectas para fines ilegales. Por eso se utilizan para pagar en el mercado negro y cada vez más en ciberataques (entre ellos, muchos de los ataques de *ransomware* ya descritos en este capítulo). El anonimato, claro está, hace que identificar a los responsables de estos ciberdelitos sea extremadamente difícil.

Por otra parte, Bitcoin también facilita el lavado de dinero criminal, ya que permite disociar los pagos de su fuente y convertir de forma anónima los bitcoins en dinero para gastar. Es decir, da la posibilidad a los delincuentes de ocultar el origen de los ingresos de las actividades ilícitas para que puedan cobrarlos de forma segura.

Pero no todo es negativo. Blockchain (o «cadena de bloques»), la tecnología tras las criptomonedas, funciona también como un sistema de seguridad y de lucha contra la falsificación. Proporciona una nueva forma de realizar y de registrar todo tipo de transacciones de forma descentralizada, transparente e inmutable, pues elimina la necesidad de una autoridad central que verifique y registre dichas transacciones. Es decir, puede operar sin necesidad de intermediarios y sin revelar datos sobre la identidad de quienes realizan las operaciones. ¿Cómo? Mediante un sistema de registro contable en forma de base de datos compartida, descentralizada y segura. Compartida y descentralizada porque hay copias en millones de ordenadores de todo el mundo, y segura porque están protegidas criptográficamente. Por eso, en teoría, no se pueden atacar, ni prohibir, ni borrar. Además, si hubiera alguna discrepancia en los registros, existe un mecanismo de consenso (que sustituye a esa autoridad central) que permite detectar cuál es el correcto.

Blockchain, como otras tecnologías, puede usarse para hacer el bien o el mal. Sin embargo, esto no significa que la tecnología sea neutra. Esta es la falacia que nos intentan vender, pues la tecnología deja de ser neutra en el momento de crearla. «Instamos —como dice el escritor James Bridle— a una cierta comprensión del mundo que, así cosificada, es capaz de lograr ciertos efectos en él. Se convierte así en otra parte de nuestra comprensión de dicho mundo, aunque a menudo de forma inconsciente.»[30]

La tecnología es producto de su tiempo y circunstancia, y del objeto de su desarrollo; reproduce los valores que la originan y es consecuencia de las elecciones políticas y sociales de cada momento. A su vez, determina, orienta y configura a su medida el mundo que le seguirá. Limita el marco de lo posible y lo no posible, e incluso la libertad de elección. Sienta las bases y los términos de las relaciones de las personas y dirige la atención humana.

Toda tecnología se diseña con un propósito. En la era de los teléfonos inteligentes, ese es el de mantener nuestra atención la mayor cantidad de tiempo posible. Engancharnos. Las redes sociales son el ejemplo más claro de una filosofía de desarrollo cuya máxima es «Cuanto más, mejor», sin importar cómo conseguirlo ni cuáles sean sus consecuencias. Las veremos en el siguiente capítulo.

4

Adicción

> *Adicción es cuando los imperativos biológicos naturales, como la necesidad de comida, sexo, relajación o estatus, se priorizan hasta llegar a la destructividad. Se ve exacerbada por una cultura que, comprensiblemente, explota esta mecánica, ya que es una muy buena manera de vender chocolatinas Mars y Toyotas.*
>
> RUSSELL BRAND,
> *Recovery. Freedom from Our Addictions*

El cómico y escritor británico Russell Brand no es un erudito, que digamos, pero se doctoró *cum laude* en abuso de heroína y en su posterior desintoxicación. Ahora abandera la causa de la rehabilitación. En su libro *Recovery. Freedom from Our Addictions*[1] habla del comportamiento adictivo más allá de la ingesta de alcohol o drogas: café, juego, comida, ejercicio, televisión, tecnología y conectividad o consumo en general. Estas, dice, se han normalizado tanto que solo son evidentes cuando se vuelven extremas. «No sabes que estás en Matrix porque estás en Matrix. Matrix es nuestra cultura de consumismo, materialismo e individualismo, que impulsa las cosas que hacemos compulsivamente para sentirnos bien: nuestras adicciones.»

El teléfono inteligente es el máximo exponente de la adicción consumista. Nos deja imágenes tan surrealistas como las interminables colas frente a tiendas de Apple en todo el mundo para comprar la última versión del iPhone. El *smartphone* diseñado por Steve Jobs no fue el primero en combinar internet y móvil (todo en uno), pero su aparición en escena en 2007 marcó un antes y un después en la adopción de estos dispositivos. La genialidad de Jobs explotó la mecánica consumista que era buena para vender no solo chocolatinas o coches, sino cualquier otra cosa.

Esta otra cosa llamada *smartphone* tenía, sin embargo, algo diferente: unía un producto portátil de bolsillo (y crecientemente accesible a todos los bolsillos) con un servicio al que ya empezábamos a ser adictos: internet. Si incluso cuando solo podíamos conectarnos a través de un ordenador la red de redes ya empezaba a ser un problema para la salud mental de muchos, poner internet en un aparato que podía acompañarnos todo el tiempo fue el paso definitivo para convertirla en el opio del pueblo.

Pese a la cantidad de fanáticos del iPhone y de otros dispositivos, lo de las colas para adquirir la versión más reciente de este dispositivo se queda en una pura

anécdota en comparación con el verdadero riesgo adictivo que conlleva. Este tiene menos que ver con el *hardware*, con el aparato en sí, que con los usos que permite ese *hardware*. Más allá de la sensación de poseer un móvil de una marca concreta, que no todo el mundo se puede permitir, la gratificación procede de lo que es posible hacer con él. Y para tener uno no es necesario gastarse cientos de euros. Muchas operadoras nos los ofrecen incluso gratis.

Para hacerse una idea de la magnitud: tres mil quinientos millones de personas, casi la mitad de la población mundial, tienen un *smartphone*.[2] En España, entre un 80 y un 96 por ciento de la población cuenta con uno de estos teléfonos,[3] lo que sitúa al país en el top 10 mundial de usuarios de estos dispositivos. Para más de un 96 por ciento de todos los internautas españoles (que son, a su vez, más de un 80 por ciento de la población), este es su dispositivo de acceso a internet. Seis de cada diez españoles consideraban en 2020 que internet y el móvil eran esenciales en sus vidas, y el 90 por ciento afirmaba que utilizaba internet a diario.

En realidad, el problema en sí no es que muchas personas tengan *smartphones* (aunque a ciertas edades resulte preocupante). La cifra que realmente asusta es esta: casi un tercio de la población española mayor de edad se consideraba adicta al móvil en 2019.[4] Es decir, más de ocho millones de personas y un total de quinientos mil adictos más que el año anterior. En 2020, sin embargo, esa cifra cayó a poco más de siete millones de personas,[5] lo que no se atribuye a una menor dependencia, sino a una mayor normalización de dicha dependencia, lo que impide apreciar la posible presencia de una adicción.

El nivel ha llegado hasta tal punto que la mayoría de la población de entre dieciocho y sesenta y cinco años (un 60 por ciento) amanece y se acuesta mirando la pantalla del teléfono. Los más jóvenes —de entre dieciocho y veinticuatro años— son los que se consideran más adictos: dedican casi siete horas diarias al aparato. Es decir, casi la mitad de las horas de actividad del día. En las cifras anteriores no se incluía a los menores de edad. En 2019, un 66 por ciento de los niños y niñas de entre diez y quince años tenían un móvil.[6] Repito: un 66 por ciento. En el caso de los quinceañeros, la cifra asciende a un 94 por ciento. En la franja de los catorce a los dieciocho años, un 20 por ciento usa internet de manera compulsiva[7] y un 18 por ciento abusa de las nuevas tecnologías.[8] Otros estudios sitúan en casi un 84 por ciento la cifra de jóvenes de entre catorce y dieciséis años que hacen un uso intensivo del móvil,[9] y en más de la mitad los que hacen un uso inadecuado, con conductas de riesgo o incluso de dependencia.[10]

Independientemente de si hablamos de adicción o no, el calibre de las cifras es innegable. Pero si entramos en faena, lo cierto es que resulta probable que no todas las personas que aseguren en una encuesta ser adictas al móvil lo sean, de igual modo que un porcentaje de las que lo niegan probablemente sí lo serán. A decir verdad, las líneas entre dependencia y adicción no siempre están claras, y la semántica juega

malas pasadas en los sondeos. Entonces ¿qué es ser adicto al *smartphone* y qué tiene el *smartphone* que genere adicción?

INTERNET

La clave está en la red de redes, en la conectividad. Muchos años antes de que se masificara el uso de los *smartphones* ya se hablaba de la adicción a internet. La psicóloga Kimberly Young fue pionera en la identificación de este trastorno. En 1995, creó el Centro para la Adicción a Internet para hacer frente al que consideraba un problema creciente. Dieciocho años más tarde, en 2013, abrió en Estados Unidos la primera clínica para pacientes con este problema, asociada al Bradford Regional Medical Center (en Pittsburgh).

La preocupación de Young tenía que ver con cómo la democratización del uso de internet había creado tanto el beneficio de la comunicación instantánea como el problema de una creciente dependencia de personas enganchadas a videojuegos y a otras aplicaciones *online*. Y eso a finales de la década de los noventa.

Young advertía ya entonces de que, si bien la adicción a internet no causa el mismo tipo de problemas físicos que otras como el alcohol, los problemas sociales son paralelos. Hablamos de pérdida de control, antojos y síntomas de abstinencia, aislamiento social, discordia matrimonial, fracaso académico, deuda financiera excesiva… Al igual que otras formas de adicción, la originada por internet consume, provoca problemas sociales, de ocupación y de relación, y, en algunos casos, arruina vidas.

Investigaciones realizadas a lo largo de más de veinte años han identificado la adicción a internet como un trastorno clínico nuevo y, a menudo, no reconocido, que afecta a la capacidad del usuario para controlar su actividad *online*. Por su tipología, se encuentra entre lo que se conoce como «adicciones sin sustancia» o conductuales. Los síntomas se comparan con los criterios utilizados para diagnosticar otros trastornos del control de impulsos como la ludopatía.

Young «metodologizó» el análisis de la adicción a internet. De acuerdo con la psicóloga, es adicto quien responda «sí» a cinco de las siguientes cuestiones:

1. Se siente preocupado por internet: piensa en su anterior actividad *online* o anticipa la siguiente sesión.
2. Siente la necesidad de utilizar internet cada vez más para lograr satisfacción.
3. Ha realizado repetidamente esfuerzos infructuosos para controlar, reducir o detener por completo el uso de internet.
4. Se siente inquieto, de mal humor, deprimido o irritable cuando intenta reducir o detener el uso de internet.
5. Permanece *online* más tiempo de lo previsto al principio.
6. Ha puesto en peligro o se ha arriesgado a perder una relación importante, un trabajo, una oportunidad educativa o profesional debido a internet.

7. Ha mentido a miembros de su familia, terapeutas u otras personas para ocultar su grado de participación en internet.
8. Utiliza internet como una forma de escapar de los problemas o de aliviar un estado de ánimo disfórico (por ejemplo, sentimientos de impotencia, culpa, ansiedad o depresión).

También hay otros síntomas, como descuidar a amigos y familiares, quitarse horas de sueño para permanecer conectado, ser deshonesto con los demás, aumentar de peso o perderlo, tener dolores de espalda o de cabeza, reducir el tiempo dedicado a otras actividades placenteras (o abandonarlas por completo), o sentirse culpable, avergonzado, ansioso o deprimido como resultado del propio comportamiento *online*.

¿Le resulta familiar alguna de las anteriores? Probablemente, más de una. La conectividad, ya sea en forma de wifi, ADSL o fibra óptica, se ha vuelto una prioridad en la pirámide de Maslow del siglo XXI. Más aún en tiempos de pandemia: seis de cada diez españoles consideran que internet y el móvil son esenciales en sus vidas, y el 90 por ciento afirma usar internet a diario.[11]

Una cosa es ser adicto a internet y otra al móvil, pero ambas se refuerzan mutuamente. Podríamos sustituir perfectamente «internet» por «*smartphone*» en todas y cada una de las cuestiones y síntomas anteriores. Su uso ha convertido la adicción a estar conectados en una epidemia. A escala mundial, las tasas de prevalencia de este trastorno que se citaban ya en 2009 variaban entre el 1,5 y el 8,2 por ciento.[12] En Europa se hablaba de más de un 18 por ciento en 2014, con cifras mayores en países como Corea del Sur, China o Estados Unidos. Es difícil encontrar cifras actualizadas y precisas al respecto, dada la falta de criterios específicos para diagnosticar este trastorno (por muy claros que parezcan los propuestos por Young, una parte de la comunidad científica los considera demasiado amplios y genéricos).

LA TRAMPA DEL *SMARTPHONE*

¿Qué tiene el *smartphone* que lo hace tan adictivo? Una explicación simple sería que condensa todo lo que nos hace ser adictos a internet en un dispositivo que, frente a las limitaciones de un portátil o de un ordenador de sobremesa, es posible llevar siempre consigo y aprovechar sus maravillas con un simple gesto manual. Se convierte en una extensión de nosotros mismos.

Entre las actividades más adictivas que ofrece, además de la conectividad 24 × 7 *per se*, están la posibilidad de acceder a información en tiempo real, las redes sociales, los videojuegos y cualquier tipo de aplicaciones y plataformas; todas ellas accesibles a través del dispositivo y con algo en común: están diseñadas para captar y mantener nuestra atención. Esto, lejos de ser algo banal, es la esencia del problema de la tecnología persuasiva. Hay toda una ciencia detrás de ello, la «captología»: el estudio de los ordenadores como máquinas de manipulación. O, lo que es lo mismo, de cómo automatizar la persuasión.

La idea nació en la Universidad de Stanford (Estados Unidos) hace algo más de veinte años, cuando el investigador B. J. Fogg acuñó el término «captología» a partir del acrónimo CAPT (*Computers as Persuasive Technologies*, «Ordenadores como Tecnologías Persuasivas»). Con él inició el estudio del poder de todos los aspectos de los productos informáticos para cambiar actitudes, comportamientos, creencias y acciones. Así se inauguró el Stanford Persuasive Technology Lab, que sentó las bases del diseño de las redes sociales, plataformas y aplicaciones que moldean el día a día de buena parte del planeta, nacidas en el imperio tecnológico de Silicon Valley.

La «captología» es más conocida hoy como «diseño del comportamiento», heredera de la psicología conductual y de las ciencias del comportamiento. En específico, de la llamada «economía conductual», cuya teoría le valió el Premio Nobel de Economía al psicólogo Daniel Kahneman.

La economía conductual o del comportamiento trata de entender cómo el ser humano toma decisiones, partiendo de la base de que no siempre lo hace de forma óptima o racional. Las personas actuamos de forma rápida e instintiva, sin pensar (demasiado). Somos animales de costumbres, y a menudo nuestro cerebro usa atajos para actuar deprisa y ahorrarnos esfuerzo. Según Kahneman, esta es la parte de nuestro Sistema 1. Este ha evolucionado para ser ultrarrápido y reacciona a señales como, por ejemplo, las normas sociales. El Sistema 2, por el contrario, es nuestro «yo» racional. Este último puede luchar contra el Sistema 1, pero ello requiere de bastante energía (fuerza de voluntad) para hacerlo, y muchas veces falla.

Este campo de conocimiento fue enriquecido por otro premio Nobel colaborador de Kahneman. Se trata de Richard Thaler, reconocido por sus investigaciones sobre cómo los aspectos emocionales y no racionales influyen en la toma de decisiones económicas y financieras. Fue la base del «paternalismo libertario», que se vale del conocimiento de la irracionalidad y de los sesgos humanos para crear un entorno que empuje a las personas a tomar mejores decisiones.

La cuestión es: ¿mejores decisiones para quién? El conocimiento de cómo actuar sobre la conducta humana para manipularla puede usarse para muchos fines. A Fogg le interesaba su aplicación a la informática, y tomó las teorías de Kahneman y de Thaler como base para desarrollar su modelo. Este se sostiene en la confluencia de tres elementos principales: motivación (querer hacer algo), capacidad (poder hacer algo) e incentivo (ser incitado a hacer ese algo). Por ejemplo, querer comprar algo, capacidad para hacerlo (tener dinero) y ser empujado a hacerlo.

De esto último se encarga el diseño de la propia herramienta, ya sea en forma de plataforma *online* o de aplicación móvil. Colores, formas, tamaños, sonidos… Todo en una web de venta *online* —como puede ser Amazon— contribuye a ese objetivo: persuadir a las personas para que compren productos una y otra vez. Captar su atención para que se queden ahí el mayor tiempo posible, ya sea comprando, compartiendo imágenes o pensamientos, interactuando con otras personas o viendo películas o series en bucle.

La «captología» cuenta con técnicas cada vez más sofisticadas y sutiles para piratear el cerebro humano y aprovecharse de sus debilidades. Cada botón y opción que se nos presenta o cada cosa que se nos recomienda o que aparece en una pantalla está justificada por las estrategias de diseño del comportamiento y sobre la base de sesgos humanos conocidos, los denominados «sesgos cognitivos» de Kahneman[*]. De acuerdo con Fogg, hay siete tipos de técnicas de persuasión particularmente adecuadas para el medio informático: reducción, tunelización, personalización, sugerencia, autocontrol, vigilancia y condicionamiento.

La reducción simplifica una tarea que el usuario está intentando realizar; la tunelización guía al usuario a través de una secuencia de actividades, paso a paso; la personalización proporciona al usuario información y comentarios en función de sus acciones; la sugerencia ofrece recomendaciones al usuario en el momento y en el contexto adecuados; el autocontrol permite al usuario realizar un seguimiento de su propio comportamiento para cambiarlo y lograr un resultado predeterminado; la vigilancia observa abiertamente al usuario para aumentar un comportamiento objetivo, y el condicionamiento se basa en reforzar o castigar al usuario para propiciar o incrementar una determinada forma de proceder, conducta o acción.

Estas estrategias se ven claramente reflejadas en sistemas que usamos a diario. El ejemplo típico es el de las redes sociales: proporcionan información personalizada, ofrecen recomendaciones en el momento y en el contexto adecuados, vigilan al usuario para aumentar su tiempo de uso y sus interacciones, y proporcionan refuerzos positivos y recompensas por el mero uso de la *app*. Para todo ello cuentan, además, con unos cada vez más poderosos algoritmos —secuencias de pasos que ejecuta una máquina— basados en tecnologías de inteligencia artificial (IA).

Los botones «Me gusta» y sucedáneos, las notificaciones, la posibilidad de etiquetar a amigos, las recomendaciones de nuevas amistades, los recordatorios de cumpleaños, la creación de grupos privados segmentados por interés, el chat instantáneo, las noticias recomendadas, las listas de tendencias o los puntos suspensivos mientras alguien escribe para que sepas que está al otro lado y no desconectes… Todo está diseñado con el objetivo de que te quedes ahí —en Twitter, en Facebook, en Instagram, en LinkedIn— la mayor cantidad de tiempo posible. Como dice el periodista Richard Seymour: «La gente nunca escribió tanto ni tan frenéticamente en toda la historia de la humanidad: enviando mensajes de texto y tuits, tecleados con los pulgares en el transporte público, actualizando su estado durante las pausas en el trabajo, haciendo pasar imágenes y pinchando enlaces frente a resplandecientes pantallas a las tres de la mañana».[13]

En las redes sociales se recompensa la inmediatez, el ingenio, el sarcasmo, la creatividad y también el despecho o el sadismo. Como constatan los científicos, la adicción que generan es muy similar a la del juego, ya que ambas están diseñadas para crear dependencias psicológicas de manera similar.

De igual modo que las tragaperras, las redes sociales buscan encerrar a los usuarios en un ciclo de adicción, ya que sus ingresos publicitarios dependen de la atención continua de dichas personas a lo que se les muestra en la pantalla. Te sumergen en círculos viciosos que incluyen incertidumbre, anticipación, impredecibilidad, retroalimentación rápida y recompensas aleatorias que animen a seguir enganchado. Y, si te desconectas, te perseguirán con mensajes o notificaciones para llamar tu atención y para que vuelvas a entrar.

Estos «bucles lúdicos»[14] que conducen a la adicción a menudo se inician por la hiperactividad del sistema cerebral que evalúa las recompensas y potencia los comportamientos impulsivos. En consecuencia, el cerebro libera dopamina, como hace cuando comemos algo rico, cuando tenemos un orgasmo o después de hacer ejercicio. Esta sustancia recompensa comportamientos placenteros y nos motiva a repetirlos. Dicha repetición puede sobresensibilizar el sistema de liberación de dopamina a partir de la sucesión repetitiva de comportamientos gratificantes con recompensas intrínsecas fuertes. Esto, a su vez, puede llevar a un estado constante de querer experimentar la conducta gratificante. Es decir, esta —ya sea consumir drogas, jugar a las tragaperras o interactuar en redes sociales— acaba volviéndose adictiva.

Todo eso lo saben bien los directivos de los gigantes tecnológicos de Silicon Valley. Tim Kendall, que fue director de monetización de Facebook desde 2006 hasta 2010, reconoció ante el Congreso de Estados Unidos que buscaban atraer tanta atención como fuera posible y que se inspiraron en las estrategias de las Big Tobacco para hacer que su aplicación fuera «adictiva desde el principio». Igual que las empresas tabacaleras decidieron incorporar azúcar y mentol a los cigarrillos para enganchar a más personas, en Facebook añadieron actualizaciones de estado, etiquetado de fotos y «Me gusta»: «Lo que hizo que el estado y la reputación fueran primordiales y sentó las bases para una crisis de salud mental adolescente».[15]

De redes sociales a videojuegos, plataformas de entretenimiento *online*, etc. Sin lugar a dudas, también puede convertirse en adictivo jugar al Candy Crush, ver contenidos en Netflix o revisar constantemente el *e-mail*, las noticias o nuestros datos de actividad en plataformas como Fitbit. En todas ellas están presentes varias de las técnicas de persuasión enunciadas antes. No es casual, por ejemplo, que, cuando llegas al final de un episodio de tu serie favorita, empiece —por defecto, de forma automática e inmediata— el siguiente. Es más difícil detener la reproducción del nuevo capítulo que seguir viéndolo.

Algo que también es común a todas las anteriores es que activan unos mecanismos y una necesidad humanos tan profunda y evolutivamente antiguos como socializar con otros, observar y ser observados.[16] Lo explica un estudio de 2018 realizado por investigadores canadienses:

> Desde una perspectiva evolutiva, la capacidad humana para funcionar de manera óptima en cualquier entorno (y de hecho la *inteligencia humana misma*) se basa en tener acceso a un gran repertorio acumulativo de información cultural contextualmente relevante ideada por

> otros, y que ningún individuo podría inventar por sí solo por su cuenta […]. Buscar noticias e información, en pocas palabras, son formas de aprender de los demás y mantenerse actualizado sobre eventos y personas culturalmente relevantes.[17]

El catedrático y psicólogo social Matthew D. Lieberman describe en su libro *Social. Why Our Brains Are Wired to Connect*[18] la necesidad de interactuar entre sí como una de las fuerzas motivadoras más fuertes que experimentan los seres humanos. Sus investigaciones en neurociencia social revelan que nuestra necesidad de conectarnos con otras personas es incluso más básica que la necesidad de comida o refugio.

De ahí que las recompensas sociales sean tan poderosas y que, de acuerdo con ello, las aplicaciones persuasivas modulen el comportamiento adictivo mediante su anticipación. Es decir, como diría una versión moderna de Kahneman, piratean nuestro Sistema 1, el de los atajos irracionales que reaccionan a señales sociales. A esto se añaden otras facetas que impactan en el hechizo tecnológico, como el aspecto sensorial (la sensualidad específica del aparato con el que nos conectamos), su forma de conectar con los deseos, sentimientos y ansiedades de cada persona o el carácter transformador de la experiencia.[19]

EL «YO» EXTENDIDO

Todas las actividades anteriores, potencialmente adictivas, son accionables desde cualquier dispositivo conectado. El más accesible de todos es, por antonomasia, el *smartphone*. Este, por su cualidad de tecnología móvil, presenta un elemento añadido para persuadir a las personas en el tiempo y el momento adecuados, lo cual aumenta las posibilidades de obtener los resultados deseados. Esto representa, según Fogg,[20] un paso adelante en la «captología» como fuente de motivación e influencia —y de manipulación— para las personas.

Al ser una compañía constante, una presencia persistente, los teléfonos inteligentes se encuentran en una situación única para persuadir. Además, se han convertido en una extensión de nuestro ser. Entran en lo que se conoce como la «teoría del yo extendido»,[21] que propone que las posesiones de un individuo, ya sea consciente o inconscientemente, de manera intencionada o no, pueden convertirse en una extensión de uno mismo.

Los *smartphones* funcionan como objetos de confort. Se han convertido en entidades tan íntimamente nuestras que son capaces de representar una extensión de nuestro yo físico; una encarnación en la que el cerebro incorpora elementos externos al esquema corporal, tratándolos como parte del propio cuerpo. Tanto es así que el 20 por ciento de la población española estaría dispuesta a implantarse un chip para sustituir al *smartphone* y sus funciones.[22]

Si el dispositivo se considera parte de uno mismo, separarse de él de forma involuntaria podría percibirse y experimentarse como una disminución del yo

extendido. De ahí la nueva fobia que emana del miedo o preocupación ante la idea de perder el móvil o de no poder usarlo: la nomofobia.

Asociada a la nomofobia surge otra patología: el FoMO (siglas en inglés de *Fear of Missing Out*, o «miedo a perderse algo»). Entran dentro de esta categoría los temores, las preocupaciones y las ansiedades en relación con estar fuera de contacto con los eventos, las experiencias y las conversaciones que ocurren *online* en nuestros círculos sociales. Es la ejemplificación de uno de los sesgos cognitivos humanos identificados por Kahneman: la aversión a la pérdida. Y eso es muy poderoso.

De ello se aprovechan las redes sociales y, entre ellas, una cuyas cuotas de popularidad se dispararon a comienzos de 2021: Clubhouse. Más allá del hecho de que solo se puede acceder por invitación (lo cual en sí genera FoMO), su funcionamiento entero está basado en FoMO, porque se basa en conversaciones en directo: quien no esté en la sala de chat en ese momento se lo pierde.

Y del FoMO al insomnio: la dependencia de esas *apps* y del móvil supone una pérdida de horas de sueño, ya sea por irse a la cama más tarde, ya sea por usar el dispositivo en mitad de la noche. Esto, a su vez, está relacionado con un aumento de la masa corporal,[23] y no precisamente muscular. Es decir: engorda.

También es conocido el efecto del uso del móvil en la alteración de los ritmos del sueño, en especial cuando usamos estos aparatos antes de dormir. La luz azul que desprenden puede influir en la producción de melatonina y, por tanto, en el ciclo circadiano. De ahí que muchos fabricantes incorporen un «modo noche» que reduce este tipo de luz de onda corta.

La idiotización es otro de los posibles efectos secundarios de pasar largas horas mirando el móvil y delegar en él un creciente número de tareas. El 46 por ciento de los españoles admite haber perdido capacidades desde que tiene un *smartphone*, el 56 por ciento no recuerda más de cuatro números de teléfono y más del 50 por ciento tendría muchas dificultades para llegar a un nuevo destino sin GPS.[24]

Otra derivada de la adicción al *smartphone* es el denominado «ningufoneo» (*phubbing*). El concepto alude al hecho de que una persona solo preste atención a un dispositivo móvil, ninguneando a las personas que la rodean y a su entorno. Es solo uno más de los efectos del *smartphone* como arma de distracción masiva. En el coche, en el trabajo, en clase… Cualquier sitio es bueno para desconectar de nuestra tarea principal y echar un ojo al móvil.

El problema de la distracción va más allá de la mera pérdida de atención: desde provocar accidentes hasta disminuir la productividad laboral, causar estrés o reducir el rendimiento académico. En España, utilizar el móvil mientras se conduce —algo que hace casi un tercio de la población— mata a trescientas noventa personas al año.[25] En cuanto a la productividad, los trabajadores reconocen que el uso personal de la tecnología en el trabajo perjudica la productividad de la organización.[26] Un estudio de 2016 cifraba la reducción del rendimiento individual en un 26 por ciento.[27]

En el ámbito académico, se ha demostrado que la mera presencia del móvil reduce la capacidad cognitiva de los alumnos.[28] Por otra parte, una encuesta realizada en seis universidades diferentes en Estados Unidos reveló que los estudiantes usan sus *smartphones* una media de once veces al día en clase.[29] Y, aunque suene muy moderno hablar de nuestra habilidad multitarea, lo cierto es que no estamos programados para realizar bien múltiples quehaceres.[30] Se ha demostrado que quienes se distraen con el móvil en clase tienden a tomar notas de menor calidad, retener menos información y obtener peores resultados en los exámenes.[31] Los propios estudiantes reconocen que usar el *smartphone* en clase disminuye su capacidad para prestar atención.[32] Incluso distrae a otros estudiantes cercanos, aunque estos no estén usando sus móviles.[33]

DE MAYOR, *INFLUENCER*

«Hijo, ¿qué quieres ser de mayor?» «Yo, *influencer*.» Más de un padre y más de una madre se habrán llevado ya las manos a la cabeza al obtener tal respuesta. Sus hijos se encuentran entre el 16 por ciento de los pequeños de entre dos y ocho años que declara que su máxima aspiración es ser *youtuber*[*] o Influencer[**][34]. Es la quinta opción profesional más atractiva para los pequeños de esa franja de edad que utilizan dispositivos electrónicos, que son la friolera de un 64 por ciento.

La escalofriante cifra va en ascenso a medida que los pequeños cumplen años, hasta llegar al 94 por ciento de quinceañeros con *smartphone*, como hemos visto al comienzo de este capítulo. La dependencia y adicción a estas edades, e incluso entre los más pequeños, es una cuestión de preocupación creciente. En 2018, Francia se convirtió en el primer país del mundo en prohibir el uso de móviles en clase. El médico y escritor francés Michel Desmurget da las claves del porqué: el uso lúdico de las pantallas perjudica todos los pilares del desarrollo, desde lo físico hasta lo emocional, pasando por lo cognitivo e intelectual.[35]

En los primeros años de vida se desarrolla el cerebro. Toda experiencia sensorial no vivida, toda interacción no producida o todo estímulo no percibido por dedicar tiempo a una pantalla serán una oportunidad perdida. Si justo en esa etapa las neuronas no reciben los «alimentos» adecuados en la cantidad correcta, no podrán aprender de forma óptima; un tiempo perdido que jamás podrá recuperarse. Por otra parte, la exposición de los menores a las pantallas fomenta su propensión a la distracción.[36] Esto afecta, entre otras cosas, a sus resultados académicos, como hemos visto antes.

Los menores de edad no son solo un colectivo particularmente expuesto a los efectos negativos de internet y el *smartphone* por su condición de personas en desarrollo, sino también por su remarcada necesidad de aceptación social. Mucho se ha documentado el uso de redes sociales por parte de adolescentes como lugar donde

buscar esa aceptación. Casi un 95 por ciento de los jóvenes españoles de entre catorce y dieciséis años tiene un perfil propio en alguna red social.[37]

Entre las redes sociales que más usan está TikTok, seguida de Instagram y Snapchat.[38] TikTok tuvo un ascenso trepidante con la llegada de la COVID-19. Aunque se supone que la aplicación no permite usuarios menores de trece años, la realidad es que carece de comprobaciones efectivas al respecto. La prueba es que una niña de diez años murió en 2021 por participar en un peligroso reto que se había popularizado en la plataforma. TikTok ha sido también cuestionada por no bloquear vídeos que promueven el ayuno y la anorexia.[39]

Los niños pasan ochenta minutos de media en TikTok, pero hay otra plataforma que la supera. Se trata de YouTube, que consume casi una hora y media de tiempo al día a los menores de entre cuatro y quince años. También pasan alrededor de una hora diaria con videojuegos. Todas estas cifras se dispararon con la pandemia.[40] Como consecuencia, los especialistas en adicciones creen que los niños se enfrentarán a una abstinencia tecnológica «épica» cuando la vida comience a volver a la normalidad.[41]

¿Qué otros efectos tiene el uso indiscriminado de estas plataformas y redes sociales entre los más jóvenes? Además de proporcionarles entretenimiento y contacto con amigos y familiares, de marcar sus sueños profesionales, de distraerles de sus obligaciones o de tener efectos indeseados, como el acoso, las estafas y los riesgos de ciberseguridad,[42] sufren también los efectos de la dependencia emocional del móvil, la adicción, las relaciones tóxicas de control, etc.[43]

Los menores someten continuamente su autoestima al juicio *online*. Lo explica muy bien Greg Lutze, cofundador de una red social llamada VSCO que no tiene ni seguidores, ni «Me gusta», ni comentarios: «Es muy difícil vivir constantemente en ese mundo donde estás todo el tiempo buscando validación en lo que piensan otras personas. Caminan entre el miedo a perderse algo y la necesidad de mostrar al mundo a alguien que no son, usando una máscara. Es sobrecogedora la presión social a la que se enfrentan. Todos la sentimos de algún modo, pero es especialmente acusada si estás creciendo y tratando de descubrir tu identidad, quién eres y cómo encajas en el mundo».[44]

Tanto es así que se relaciona con las redes sociales el agravamiento de problemas de ansiedad, depresión o sensación de aislamiento social en estas edades. Usan estas aplicaciones para calmar sentimientos de culpa, ansiedad, inquietud, desamparo o depresión, o para olvidarse de problemas personales y, paradójicamente, acaban experimentando angustia, ansiedad y síntomas de depresión debido a ellas.[45] Muestran una devoción extrema por las redes sociales en detrimento de las relaciones interpersonales, lo cual desemboca en problemas familiares, concentración y colaboración deterioradas y conflictos sociales como la pérdida de amigos.

No todo es negativo, sin embargo. Más bien, la dosis hace el veneno, como dijo Paracelso. El uso frecuente de las redes sociales en la infancia se asocia a un peor bienestar y a una angustia psicológica, pero su uso poco frecuente también se vincula

a un menor bienestar.[46] Ello hace pensar que la participación de los menores en redes sociales puede ser un indicador de su participación social general, que es un factor importante para el bienestar.

Más allá de las redes sociales, el uso excesivo de las pantallas por parte de niños y adolescentes se relaciona con una larga lista de efectos. Entre ellos: sueño deficiente y factores de riesgo de enfermedades cardiovasculares, problemas de visión y reducción de la densidad ósea, síntomas depresivos y suicidas, comportamientos relacionados con el trastorno por déficit de atención e hiperactividad (TDAH), riesgo de comportamiento antisocial y una disminución del comportamiento prosocial, actitudes de deseo similares a la dependencia de sustancias o cambios estructurales del cerebro relacionados con el control cognitivo y la regulación emocional.[47]

Consciente de ello, el Gobierno español aprobó en 2018 la primera Estrategia Nacional de Adicciones, que incluía actuaciones frente a la adicción a las nuevas tecnologías y al juego. Por su parte, las redes sociales siguen intentando captar adeptos entre la generación Z.[48] Una generación que, por cierto, ya prefiere estas plataformas a las discotecas.[49]

OBJETORES DE CONCIENCIA

Sabiendo lo que ahora sabemos, no es de extrañar que los capos de los gigantes tecnológicos de Silicon Valley restrinjan al máximo el tiempo de exposición de sus hijos a las pantallas de *smartphones*, tabletas u ordenadores de cualquier clase, o que controlen y limiten su acceso a internet, o que retrasen la edad a la que les permiten tener un móvil.[50]

Por algo los mandamases de Facebook, Google, YouTube, Snapchat, Apple o Microsoft —de esas aplicaciones, videojuegos, plataformas y redes sociales adictivas — protegen de la tecnología a sus vástagos. Por algo era precavido Steve Jobs y lo son ahora Bill Gates o Sundar Pichai. Por algo el cofundador de Twitter, Jack Dorsey, abandera la causa de la desintoxicación y la desconexión digital. Por algo Tristan Harris, exempleado de Google, especialista en ética del diseño y filósofo de producto, decidió abandonar el barco y crear el Center for Humane Technology,[51] una iniciativa contra la manipulación de la tecnología persuasiva y en favor de un desarrollo y uso responsable de la tecnología. Por algo tantos otros altos ejecutivos de los gigantes tecnológicos de Silicon Valley se declaran objetores de conciencia contra las plataformas sociales.

El propio Fogg, creador del diseño conductual, parece más preocupado ahora por limpiar su nombre y autojustificarse. Dice que siempre ha insistido en que su objetivo con la «captología» era y es ayudar a las personas a conseguir hacer lo que quieren hacer. Un enfoque que, de hecho, aplicaron también la Administración Obama y el Reino Unido, cuyos gobiernos oficializaron en 2010 su trabajo en «Gobierno

conductual» para aplicar las ciencias del comportamiento al diseño de sus políticas y programas.

Fogg renombró su laboratorio, que ahora se llama Behavior Design Lab, para deshacerse de la palabra «Persuasive» que tan mala fama le traía. Ahora está desarrollando herramientas como Screentime para ayudar a las personas a reducir el tiempo que pasan delante de una pantalla. En 2019, predijo la emergencia de un movimiento para ser «posdigital». «Empezaremos a darnos cuenta de que estar encadenado al teléfono móvil es un comportamiento de bajo estatus, similar al tabaquismo», dijo en Twitter.

El inventor de la «captología» fue, por cierto, maestro de Harris. Ambos promulgan ahora los perjuicios de la tecnología persuasiva carente de ética. Ni uno ni otro abogan por dejar de usar la tecnología, sino por «hacer que la industria cambie y ponga nuestros intereses en primer lugar», dicen. ¿Son parte del *statu quo*?, ¿unos oportunistas de la causa de la tecnología ética que ahora parece estar de moda? ¿Pretenden simplemente convertirse en gurús a los que hay que seguir para, de paso, capitalizar el discurso en torno al tema y silenciar visiones más críticas o, al contrario, aprovecharán su visibilidad para contribuir de forma significativa al cambio? Es algo que está por ver, más allá de discursos biensonantes o documentales bienintencionados, como *El dilema de las redes sociales* (2020), que ensalzan la propia figura de sus impulsores.

Como ellos, otros han seguido caminos similares. Nir Eyal, conocido por su superventas *Enganchado (hooked). Cómo construir productos y servicios exitosos que formen hábitos*, ahora engrosa sus arcas con un nuevo libro sobre cómo liberarnos de esa misma adicción. Es un truco recurrente en el sector tecnológico: primero crean el problema y después nos venden las soluciones a ese problema que antes no teníamos.

Pero ¿por qué lo hacen? ¿Por qué los gigantes tecnológicos y las empresas de la esfera de las redes sociales y las plataformas, de los videojuegos y de las aplicaciones *online*, han basado el diseño de sus productos en la persuasión? ¿Por qué su propósito de engancharnos y mantener nuestra atención? La respuesta es clara: porque es su manera de hacer dinero, de ser rentables. Es su modelo de negocio, un modelo que nace como reacción a una realidad: que la gente espera que internet y todo lo que hay en él sea gratis.

La gratuidad y la visión de internet como un espacio democrático, abierto, libre y liberador —tan maravilloso como suena— son los pecados originales de internet. Es lo que ha hecho inmensa a la red de redes, para bien y para mal, con sus virtudes y defectos, cuyas consecuencias estamos viendo hoy. De ello hablaremos extensamente en el capítulo 8. Es momento, ahora, de ahondar en otro efecto esperpéntico del modelo de negocio predominante *online* y de la explotación de lo peor del ser humano. Nos referimos a la desinformación y el discurso de odio que empiezan a

socavar las democracias. ¿Cómo y hasta qué punto? Lo descubriremos a continuación.

5

Desinformación y odio

> *El objetivo de la propaganda actual no es solo desinformar o promover un determinado plan. Es agotar tu pensamiento crítico, aniquilar la verdad.*
>
> GARRI KASPÁROV, Gran Maestro de ajedrez, autor, activista y político

> *El uso de la propaganda es antiguo, pero nunca antes había existido una tecnología para difundirla con tanta eficacia.*
>
> NATALIE NOUGAYRÈDE, periodista francesa columnista de *The Guardian*

La historia comienza con un nombre: Edward L. Bernays. Fue el hombre que convirtió el beicon con huevos en el desayuno norteamericano por antonomasia, cuando la mayoría de la población apenas comenzaba el día con un café, un zumo de naranja y, si acaso, un panecillo. Convenció a los estadounidenses preocupados por consumir demasiado alcohol de que la cerveza era la «bebida de la moderación». Puso un reloj en la muñeca de los hombres que pensaban que llevar un brazalete era cosa de mujeres. Y utilizó al movimiento feminista para asociar el acto de fumar cigarrillos —«las antorchas de libertad»— a un gesto de liberación femenina.

Por supuesto, Bernays también empleó su conocimiento en política. Por ejemplo, para planear el derrocamiento, en 1954, del Gobierno socialista de Juan Jacobo Árbenz Guzmán en Guatemala; o para ayudar a blanquear la participación de Estados Unidos en la Primera Guerra Mundial con la idea de que el único propósito de la Administración Wilson[1] era llevar la democracia a Europa.

Como buen sobrino de Sigmund Freud, Bernays utilizó los postulados del psicoanálisis para desarrollar la «teoría de la propaganda» y crear el concepto de «profesional de las relaciones públicas». El austriaco, nacido en 1891, asesoró a varios presidentes de Estados Unidos y a decenas de multinacionales como Lucky Strike, Procter & Gamble, General Electric o General Motors, además de a medios de comunicación como la CBS o la NBC. Su primer libro, *Cristalizando la opinión pública*,[2] le sirvió de inspiración al alemán Goebbels, el que fuera ministro de Propaganda del Tercer Reich.

No es que Bernays fuera el primer propagandista de la historia, pero fue pionero en convertirla en algo con aspecto de ciencia: el nuevo campo de las «relaciones públicas». Utilizó los principios psicoanalíticos para moldear su concepto de «ingeniería del consentimiento» como materialización de su hipótesis de que, al

entender la mente colectiva, por qué y cómo actúan las personas como individuos y como grupo, sería posible manipular su comportamiento sin que estas se dieran cuenta.

Con ello, sentó las bases para la manipulación organizada de las masas por parte de gobiernos y corporaciones. Tal y como él mismo explicaba:

> La ingeniería del consentimiento es la *esencia misma* del proceso democrático, la libertad de persuadir y sugerir. Las libertades de expresión, prensa, petición y reunión, las libertades que hacen posible la ingeniería del consentimiento, se encuentran entre las garantías más apreciadas de la Constitución de Estados Unidos. La ingeniería del consentimiento debe basarse teórica y prácticamente en la comprensión completa de aquellos a quienes intenta conquistar. Pero a veces es imposible llegar a decisiones conjuntas basadas en el entendimiento de los hechos por parte de todas las personas. El adulto estadounidense promedio tiene solo seis años de escolaridad a sus espaldas. Con crisis urgentes y decisiones a las que hacer frente, un líder no puede muchas veces esperar a que la gente llegue a un acuerdo general. En ciertos casos, los líderes democráticos deben desempeñar su papel en la conducción del público mediante la ingeniería del consentimiento hacia metas y valores socialmente constructivos. Este rol les impone naturalmente la obligación de utilizar medios educativos, así como otros disponibles, para lograr una comprensión lo más completa posible. **[3]**

O, hablando en plata: «Como el americanito medio es analfabeto [o lo era, según él, en aquella época], necesita que nosotros los ilustrados le persuadamos para guiar sus decisiones en la dirección correcta». Unas palabras igual de insultantes que su calificación de este método como «esencial» en una democracia y su torticera vinculación con las libertades de prensa, expresión o reunión. Una forma redonda, eso sí, de legitimar la manipulación. Ese fue su principal empeño, que había plasmado años atrás en su obra más conocida, *Propaganda*:

> La manipulación consciente e inteligente de los hábitos organizados y las opiniones de las masas es un elemento importante en la sociedad democrática. Quienes manipulan este mecanismo invisible de la sociedad constituyen un Gobierno invisible que es el verdadero poder gobernante de nuestro país.
> Somos gobernados, nuestras mentes están moldeadas, nuestros gustos formados, nuestras ideas sugeridas, en gran parte por hombres de los que nunca hemos oído hablar. Este es un resultado lógico de la forma en que se organiza nuestra sociedad democrática. Un gran número de seres humanos deben cooperar de esta manera si quieren vivir juntos como una sociedad que funciona sin problemas.**[4]**

Así justificaba Bernays, con un descaro pasmoso, ni más ni menos que la necesidad y el deber de ser manipulados por nuestro bien y el de la sociedad. Así naturalizó, instauró y generalizó el diseño de la opinión de masas. Para ello elaboró una metodología cuyo punto central era el conocimiento del público y de sus diferentes subgrupos: ¿cuáles son las actitudes de las personas hacia la situación que le preocupa al ingeniero del consentimiento? ¿Cuáles son los impulsos que gobiernan estas actitudes? ¿Qué ideas consiente absorber la gente? ¿Qué están dispuestos a hacer si se les estimula de forma eficaz? ¿Qué líderes de grupo influyen en el proceso de pensamiento de qué seguidores? ¿Cuál es el flujo de ideas, de quién a quién? ¿En

qué medida la autoridad, la evidencia fáctica, la precisión, la razón, la tradición y la emoción juegan un papel en la aceptación de estas ideas?

Para responder a estas preguntas, sería necesario realizar minuciosos estudios, cuestionarios, entrevistas, contacto con los líderes de opinión de cada grupo formal (por ejemplo, sindicatos, asociaciones profesionales, confesiones religiosas, etc.) e informal (definido por cualquier aspecto en común, como puede ser leer *The NewYork Times* o escuchar jazz). Ello revelaría motivos subconscientes y conscientes en el pensamiento público, así como las acciones, palabras e imágenes por las que se ven afectadas. El resultado sería para el ingeniero del consentimiento el equivalente a lo que el plano es para el arquitecto o el mapa para el viajero: su hoja de ruta.

Cuando murió en 1995, con ciento tres años, el maestro de la propaganda no podía atisbar hasta qué punto internet sería para su teoría el santo grial: el sueño de la hiperpersonalización hecho realidad, al menos, en apariencia. Desde la posibilidad de rastrear la secuencia de clics de cada individuo hasta nuevos canales de escucha (o vigilancia) y acceso, pasando por la recopilación masiva de datos (el big data), todo ello potenciado por sistemas de inteligencia artificial. La maquinaria perfecta para la manipulación.

La hiperpersonalización utiliza todas estas herramientas para tratar de adaptar a cada individuo, cual traje a medida, el contenido de las campañas de influencia y marketing. Se utilizan para vender y para convencer; para inducir al consumismo y para atraer a las personas a cualquier tipo de causa, ideología, movimiento o partido.

Ahora juntemos la hiperpersonalización y la «captología» y tendremos el cóctel perfecto para los ingenieros del consentimiento: un montón de gente que pasa un montón de tiempo *online* recibiendo contenido personalizado, ya sea en forma de sugerencia de web que hay que visitar, de artículos o vídeos en los que hacer clic, de mensajes o actualizaciones en redes sociales, o de anuncios. Horas y horas expuestos al bombardeo constante de impactos y estímulos que nos incitan a comprar lo que saben que queremos comprar y a pensar lo que quieren que pensemos.

Un completo ecosistema diseñado para estimular y manipular la psique humana, para atraernos y persuadirnos de que cambiemos qué y cómo compramos, votamos, comemos o hacemos ejercicio, o a quiénes seguimos, odiamos, admiramos y adoramos. Un ecosistema del que se benefician desde los vendedores y las grandes marcas hasta los partidos políticos y los *crackers*, pasando por todo tipo de troles y promotores de la «conspiranoia». Todos esperan cambiar la forma en que pensamos y actuamos, por lo que su influencia lo impregna todo.

DE CLEOPATRA A LOS *HACKERS* RUSOS

¿Qué es y dónde entra aquí la desinformación? Se trata de información verificablemente falsa o engañosa creada, presentada y difundida con fines de lucro económico o para engañar intencionadamente al público.[5] Es un tipo de contenido

que ningún medio de comunicación periodístico al uso publicaría tras su debida labor de verificación.

A veces, esta clase de noticias no son fácilmente desmontables. Tras una certeza —un gancho— esconden una mentira. Otras simplemente toman pequeñas porciones de una realidad que aparece exagerada y distorsionada.[6] Su mayor peligro reside en que se disfrazan de verdad para parecer verosímiles y, a menudo, el engaño pasa desapercibido.

Hablamos de desinformación en internet por el factor multiplicador de la red de redes, no solo por su alcance y escala masiva, sino por el funcionamiento intrínseco de los motores de búsqueda y recomendación, las plataformas de autopublicación y las redes sociales, que premian este tipo de contenido y lo hacen más visible. Ello ha hecho de este un fenómeno exponencial, pero la desinformación existió mucho antes que internet, asociada a la propaganda.

Como decíamos, Bernays no fue el primero en ejercitar las técnicas propagandísticas. Su historia se remonta al año 515 a.C., con la llamada «inscripción de Behistún», realizada en la pared de un acantilado en Irán. En ella se cuentan, en tres lenguas diferentes, las hazañas de Darío I de Persia previas a su acceso al trono.[7]

Más adelante, el militar griego Temístocles (525-460 a.C.) usó la propaganda para retrasar la acción y derrotar a su enemigo, Jerjes. Por su parte, Alejandro Magno (356-323 a.C.) puso su imagen en monedas, monumentos y estatuas. Pero quienes más avanzaron en esta técnica fueron los emperadores romanos, que usaron variadas estrategias para influir en la opinión pública: desde el patrocinio hasta el juego de roles, la genealogía, la iconografía o la rumorología y la desinformación. A César Augusto (63 a.C.-14 d.C.) se le atribuye la difusión de información falsa como estrategia propagandística. Por ejemplo, con la descripción histórica de Cleopatra como una astuta seductora, con el pretexto de proteger a Roma de la decadencia moral y en pro del retorno a los valores familiares «adecuados».[8]

La rumorología, los bulos, las noticias engañosas y las medias verdades forman parte del arsenal de la desinformación. Por su presencia actual en nuestras vidas, cualquiera diría que es un problema del siglo XXI. Pero no, se trata de una táctica frecuentemente usada con fines propagandísticos desde hace miles de años. Sin embargo, mucho ha cambiado desde el siglo VI a.C. La propaganda y la desinformación han tenido tiempo de evolucionar, de perfeccionarse y de adaptarse a los tiempos mediante nuevas estrategias, herramientas y tecnologías. Internet es, entre todas ellas, la reina madre.

¿Quién podría imaginar hace unos años que piratas informáticos rusos podrían interferir en las elecciones estadounidenses? No es que a nadie le extrañe que Rusia trate de influir en los resultados electorales en Estados Unidos, pero nunca hasta ahora había contado con armas para hacerlo de forma tan eficiente y a tal escala. Esa eficiencia y escala, son las ventajas de la propaganda informatizada. Lo que hace

menos de una década hubiera parecido impensable no resulta hoy extraño: cualquier país puede ser víctima del ejército de la desinformación *online*. Un ejemplo claro de cómo el afán por computarizarlo todo se nos ha ido de las manos.

Las preocupaciones sobre las noticias falsas comenzaron a raíz de las elecciones presidenciales de Estados Unidos en 2016. Aquello fue solo un primer bocado de lo que se venía cociendo a fuego lento en internet. Como se suele decir, la red de redes amplifica lo bueno y lo malo, y en este caso no iba a ser diferente. Desde sus comienzos, ha sido el caldo de cultivo perfecto para la infodemia y la epidemia de troles, memes, bots, vídeos y artículos desinformativos y *deepfakes*: los principales componentes de la guerra de la (des)información.

TROLES: EL PRÓXIMO ERES TÚ

> *¿Qué es un trol?, dices mientras clavas*
> *en mi pupila tu pupila azul.*
> *¡Qué es un trol! ¿Y tú me lo preguntas?*
> *Un trol… eres tú.*[9]

En la mitología escandinava, los troles son seres gigantes y monstruosos que viven en las montañas, en castillos o bajo puentes, que son hostiles a los seres humanos o violentos con ellos, y que solo salen al anochecer. En el entorno digital esos personajes son personas de carne y hueso que también actúan con más frecuencia por la noche y adoptan una actitud poco amigable. Promueven el odio. Intervienen en foros digitales con el objetivo malintencionado de generar polémica, ofender, molestar, cansar, enfadar, tomar el pelo, vacilar, gastar una broma pesada y/o provocar a los demás usuarios.[10] Lo hacen enviando multitud de mensajes que pretenden captar la atención e impedir el intercambio o desarrollo habitual de dicho foro.

Un trol *online* es la versión cibernética del cuñado tocapelotas, del primo graciosete o del colega burlón. Podría ser, en realidad, cualquiera de nosotros. Todos somos troles *online* en potencia. Solo es necesario que se dé la situación adecuada. Un clic que haga saltar la liebre. Es la conclusión —que puede resultar obvia— de un estudio de las universidades de Stanford y Cornell (Estados Unidos).[11]

Aunque a menudo vemos a los troles como sociópatas, personas diferentes al resto de nosotros, en las circunstancias adecuadas cualquiera puede convertirse en uno de ellos. Ello depende, sobre todo, del estado de ánimo. Una persona que se despierta de mal humor puede detonar una cascada de troleo e incitar a otros troles, que, al recibir respuestas contrarias o votos negativos, son más propensos a seguir comentando y a hacerlo cada vez en peores términos. La negatividad genera negatividad, de igual modo que el odio incita al odio, hasta llegar incluso a lo delictivo. A menudo, los troles instigan un tipo de discurso del odio que promueve la discriminación o la violencia contra cualquier persona o grupo, ya sea por razones de género, raza, religión, discapacidad u orientación sexual.

Este tipo de comportamiento se da también fuera de la red, pero las características de internet contribuyen a facilitarlo. El anonimato *online* se asocia a una proliferación del mal comportamiento en los espacios compartidos, ya que desindividualiza y reduce la responsabilidad. Este efecto de desinhibición sugiere que en entornos *online* es más fácil incentivar a las personas a actuar de manera antisocial.

Tanto es así que ha dado lugar a una subclase de troles: los *sockpuppets*. Un *sockpuppet* es un muñeco de trapo, una marioneta (*puppet*) hecha con un calcetín (*sock*). En su versión *online*, los *sockpuppets* son una raza de impostores que crean cuentas títere. Es decir, cuentas falsas con las que a menudo se infiltran en otras comunidades *online* para difundir desinformación. Buscan persuadir desde dentro, y también conocer mejor a su público objetivo o a sus adversarios.

EJÉRCITO (RO)BOT

En apenas un día, Tay alabó a Hitler, promovió el nazismo y el odio contra los judíos, atacó a las feministas, lanzó mensajes transfóbicos y anunció la construcción de un muro con México. Tay podría ser un trol humano, pero no lo era, ni era el propósito de sus creadores que se convirtiese en algo ni remotamente parecido. Sin embargo, este bot basado en inteligencia artificial pasó a la posteridad por sus mensajes de odio y discriminación en Twitter. Fue creado por Microsoft como un experimento para comprobar hasta dónde llegaba la capacidad de un robot virtual para aprender de su interacción con los usuarios de dicha red social, que fue capaz de corromper al bot en menos de veinticuatro horas. Todo un éxito.

Los bots son programas informáticos que funcionan automáticamente y que realizan distintas tareas, desde buscar y encontrar información en internet hasta ejecutar comandos, responder o difundir mensajes o imitar conductas humanas. En sus múltiples tipos y formas, estos robots virtuales son ya parte de nuestros inseparables de la fauna *online*.

Los hay buenos y malos, tontos y menos tontos. Se emplean a menudo en forma de chatbot para resolver dudas de clientes o ayudarles con alguna incidencia. Son los típicos y a veces tediosos asistentes virtuales. También se usan como herramienta informativa. Por ejemplo, organismos como la Organización Mundial de la Salud (OMS) y diferentes administraciones públicas crearon bots oficiales para informar sobre la evolución de la pandemia de la COVID-19, proporcionar recomendaciones y resolver dudas frecuentes. Los bots tienen asimismo aplicaciones transaccionales, como agentes que actúan en nombre de los humanos para completar intercambios financieros o comerciales.

En el lado oscuro están los bots maliciosos, con una omnipresencia creciente; tanto que ninguna industria está a salvo de su actividad.**[12]** Estos bots interactúan con las aplicaciones de la misma manera que lo haría un usuario legítimo. Entre estos hay bots *cracker*, creados para distribuir programas maliciosos, engañar a personas o

atacar sitios web o diferentes redes; bots *scraper*, diseñados para robar contenido de sitios web; bots *spammers* o *spambots*, que publican contenido promocional de mala calidad en la web, y bots personificadores, que imitan las características naturales del usuario.

Estos últimos, los personificadores —sistemas automatizados que adoptan la forma de cuentas de usuarios humanos para difundir contenido *online* de modo constante, cientos de veces al día—, son los más controvertidos. Se les atribuyen fines propagandísticos y el estar diseñados para influir en la opinión pública o invisibilizar opiniones políticas contrarias o de disidentes. Por ejemplo, durante la campaña presidencial de 2012 en México se hablaba de los «peñabots» para referirse a un ejército de bots creado para promover en redes sociales la figura del entonces candidato Enrique Peña Nieto, apoyar su discurso e imagen y acallar las críticas contra él.

Tras la victoria de Peña Nieto, se atribuyó también a los «peñabots» las campañas de desprestigio contra activistas y periodistas como Lydia Cacho, reconocida internacionalmente por sus investigaciones contra abusos y violencia sexual, tráfico infantil y pornografía; también las estrategias de silenciamiento de sucesos como el «caso Iguala» por la desaparición en 2014 de cuarenta y tres estudiantes y otros tres muertos y veinticinco heridos en una aldea del estado mexicano de Guerrero.

Los «peñabots» no eran nada sofisticados: se limitaban a repetir mensajes con diferentes propósitos. Y no está claro si realmente eran bots o cuentas falsas manejadas por personas que copiaban y pegaban los mismos mensajes según tocara. También podrían ser bots cíborg: cuentas híbridas que funcionan como bots, pero que de vez en cuando una persona controla para interactuar con otros usuarios y publicar contenido original, de modo que no sea tan obvio que se trata de un bot.

La existencia de este tipo de bots «sociales» está siendo discutida. Revisiones de cuentas que se han contabilizado en estudios como «bots sociales» han concluido que en realidad estaban «indudablemente operadas por usuarios humanos […] sin el más mínimo rastro de automatización».[13] Hay, por tanto, un alto riesgo de falsos positivos, sobre todo si la única forma de hacer el recuento es a través de herramientas de detección automatizadas que se basan en reglas generales, sin comprobación manual humana.

«OLA K ASE», MEME

Están en todas partes. Todo el mundo ha recibido un meme en WhatsApp o lo ha visto en Twitter, Facebook o Instagram. ¿Se acuerdan de la famosa llama del «ola k ase»? Eso era un meme. Como ese, miles de ejemplos plagan las aplicaciones de mensajería, foros *online* y redes sociales.

La pandemia de la COVID-19 ha traído todo un arsenal de memes: fotos de políticos usadas fuera de contexto, que los parodian o añaden mensajes que los

ridiculizan; frases mordaces o tontas escritas en dibujos animados, o simples bloques de texto en formato imagen o vídeo corto. Suelen tener numerosas variaciones: muchas versiones de la misma imagen con un determinado personaje común, pero distintos textos.

Los memes son un elemento de diversión, de mofa (a veces hiriente), que puede servir para pasar un buen rato o para quitarle hierro a algún asunto. Sin embargo, no son inofensivos. O no lo son siempre. Su origen, o más bien el de su definición, se remonta a 1976. Lo conceptualizó el biólogo evolutivo Richard Dawkins como una unidad de transmisión cultural que cumple un papel similar en la evolución cultural al que desempeña un gen en la evolución biológica.[14] Designa un producto que se reproduce y difunde rápido —por imitación— en una determinada cultura.

Etimológicamente, «meme» viene del griego *mimema,* que significa «cosa que es imitada». Son dispositivos retóricos en los que el argumento se realiza a través de la ausencia de la premisa o conclusión.[15] Como tales, se convierten en una fabulosa arma de desinformación que puede usarse con objetivos estratégicos.

Explica la investigadora de Harvard Claire Wardle que las referencias en las que se basan los memes (un evento noticioso reciente, una declaración de una figura política, una campaña publicitaria o una tendencia cultural) no se detallan, lo que obliga al espectador a conectar los puntos. Este trabajo adicional atrae al individuo, que siente que está conectado con los demás.

Vemos de nuevo cómo reacciona aquí el Sistema 1 definido por Kahneman, el de los atajos irracionales que reaccionan a señales sociales.[16] Es una forma de actuar movida por la anticipación de recompensas sociales, como el sentido de pertenencia. Además, la naturaleza aparentemente lúdica de este formato lo hace muy compartible. Esto convierte a los memes en vehículos influyentes para la desinformación, la conspiración o el odio. No requieren hacer clic en un enlace externo, ni deslizarse por la pantalla para verlo o leerlo todo, ni ningún otro esfuerzo adicional: todo lo que transmite está a simple vista y adaptado a la pantalla del *smartphone*.

DESINFORMA, QUE ALGO QUEDA

«Hacer gárgaras de sal ayuda a combatir el coronavirus.» «Un niño de seis años ha muerto por llevar mascarilla.» «La pandemia de la COVID-19 está causada por el 5G.» «Bill Gates ha confirmado que van a plantar chips en la vacuna contra el coronavirus.» «Italia ha encontrado la cura contra la COVID-19.» «Tomar café previene el coronavirus.» «Pedro Sánchez recomienda invertir en Bitcoin para generar ingresos mientras dure la pandemia.»[17]

Los titulares anteriores pueden resultar ridículos, pero lo cierto es que hay gente ahí fuera difundiéndolos como ciertos, y creyendo y haciendo creer a otros que en efecto lo son. Los bulos se duplicaron en España un mes después del estado de

alarma.[18] Es un hecho que el aluvión de noticias falsas, bulos y desinformación ha sido significativamente mayor en esta pandemia en comparación con eventos similares en el pasado, incluso con campañas electorales o desastres naturales. Antes se usaban tal vez media docena de historias de desinformación que circulaban de distintas maneras, y ahora hay centenares. Además, no son solo locales, sino globales.[19]

Si los memes se benefician de su disfraz de broma para difundirse, las falsedades, bulos, noticias fabricadas e informaciones engañosas se visten de aparente verdad para correr como la pólvora. Circulan en forma de vídeo, audio o texto que cualquiera puede crear. Por lo general, se caracterizan por titulares llamativos o sensacionalistas que buscan el clic fácil (los ciberanzuelos) y el uso engañoso de imágenes, gráficos, datos o información fuera de contexto.

A menudo este tipo de desinformación contiene palabras en mayúscula e incluso errores ortográficos. En otros casos el contenido es totalmente falso y manufacturado, con apariencia seria, satírica o de parodia, verosímil o no. O a veces trata de parecer verídico mediante el uso de simbología asociada a un medio de confianza, por ejemplo, alojándose en sitios web con direcciones parecidas —pongamos por caso, <www.elpais.net> en lugar de <www.elpais.com>— y usando un logotipo, un diseño visual, una tipografía y un estilo similares.

Otro fenómeno es el de los *deepfakes*, a los que llamo «falsificaciones hiperrealistas». Son creaciones digitales parcial o totalmente ficticias que distorsionan, manipulan y/o imitan la voz y/o la imagen (foto o vídeo) de personas reales, o que usan sonidos e imágenes para crear figuras aparentemente humanas. Para ello se emplean técnicas de inteligencia artificial cada vez más sofisticadas. Uno de los primeros *deepfakes* virales fue un vídeo del expresidente estadounidense Barack Obama diciendo que Trump «es un total y completo imbécil». En realidad, era otra persona la que decía eso, pero la tecnología Face2Face permitía sincronizar los movimientos faciales de aquella con una imagen de la cara de Obama y con su tono de voz, de tal forma que pareciera que era este último el que hablaba.

El falso vídeo de Obama fue creado en 2018 por el medio estadounidense *Buzzfeed* con el propósito de poner de relieve el potencial manipulador de los *deepfakes*. Desde entonces se han sucedido los ejemplos: aplicaciones con las que rejuvenecer, envejecer, cambiar de sexo o convertirse en una celebridad; herramientas que permiten dar vida a fotos antiguas o que imitan voces de personalidades; webs como <www.thispersondoesnotexist.com> que producen imágenes de personas ficticias a partir de miles de fotografías de rostros humanos; creaciones pornográficas… La tecnología ha mejorado tanto que ya no requiere de expertos: cualquiera puede hacer una de estas falsificaciones desde su móvil sin ningún conocimiento técnico.

El problema es monumental, porque la democratización de la creación de *deepfake*s multiplica la producción de contenido falso que cada vez es más difícil de

distinguir de la realidad. Más desinformación y más estafas. La tecnología ya se ha cobrado más de una víctima, como el director de una empresa de energía del Reino Unido, que transfirió doscientos veinte mil euros a unos delincuentes que se hicieron pasar por su superior falseando su voz por teléfono.[20]

También se han utilizado *deepfakes* para adulterar y vender imágenes de supuestos desnudos de celebridades o menores de edad,[21] o para difamar a periodistas críticas con sus gobiernos.[22] Además, se ha descubierto la creación de porno *deepfake* a partir de fotografías de mujeres reales desnudas provenientes de sitios web acusados de trata de blancas, coerción y violación.[23]

Uno de los efectos más peligrosos de estos sistemas es la sensación de incertidumbre sobre qué es cierto y qué no, en un contexto en el que cualquiera puede crear estos contenidos. Ello puede incluso conducir a un golpe de Estado, como sucedió en Gabón.[24] Debido a un problema de salud, su presidente Ali Bongo pasó un tiempo sin aparecer públicamente, lo que generó rumores sobre su muerte. Cuando volvió, lo hizo mediante un vídeo, y la oposición hizo correr la idea de que en realidad era falso. Los rumores de una conspiración se viralizaron en las redes sociales, la situación política se desestabilizó y los militares dieron un golpe de Estado, todo en el breve intervalo de una semana. Aunque no se sabe con seguridad si el vídeo era falso, los expertos creen que no. De hecho, Bongo ha vuelto a aparecer en público y sigue siendo presidente de Gabón.

Los *deepfakes* no solo se utilizan para manipular, desinformar o estafar. También se usan para entretener o como gancho publicitario. Un ejemplo: el anuncio de una marca de cerveza que devolvió a la vida a Lola Flores. Como era de esperar, corrió como la pólvora por redes sociales y por aplicaciones de mensajería. El funcionamiento de estas plataformas facilita la viralización masiva de contenido falso, independientemente de que tenga un propósito lúdico o malicioso. Encuentra tirón en un tipo de distribución por «redes de confianza» entre pares: familiares, amigos, conocidos, grupos de WhatsApp o Facebook, seguidores en redes sociales y un largo etcétera.

Este tipo de distribución aumenta la probabilidad de que la desinformación se comparta y se viralice, y más aún si el contenido tiene un componente emotivo.[25] Además, una vez que una falsedad empieza a expandirse, no hay quien la pare, ni posibilidad de eliminarla de la faz de internet, aunque haya iniciativas poniendo medios para frenar su difusión o, al menos, desmentirla.

INFODEMIA E INFOXICACIÓN

Vivimos tiempos de pandemia. Hay una que llegó para quedarse mucho antes que la COVID-19: la infodemia. El término puede ser entendido de varias formas. Una es la propagación epidémica de desinformación, noticias falsas y teorías de la conspiración. Interfiere con el suministro de información y la toma de decisiones que

es de crucial importancia tanto para los políticos y los organismos gestores de crisis como para los ciudadanos. Es algo que redes sociales como Facebook han facilitado a sabiendas: «Permitir que floreciera la información errónea, las teorías de la conspiración y las noticias falsas se asemejaba a los broncodilatadores de Big Tobacco, que permitían que el humo del cigarrillo cubriera más superficie de los pulmones», aseguró frente al Congreso estadounidense Tim Kendall, el exdirectivo de Facebook anteriormente mencionado.[26]

Otra forma de definir «infodemia» es la de la OMS: «Demasiada información —incluida información falsa o engañosa en entornos digitales y físicos— durante el brote de una enfermedad».[27] Incluso habla de toda una disciplina científica: la «infodemiología». En torno a ella trabaja este organismo para crear herramientas que las autoridades de salud y las comunidades puedan utilizar para prevenir y superar los impactos dañinos causados por las infodemias. Sobre todo mediante alfabetización digital y sanitaria.

La tercera «acepción» de infodemia se refiere a la sobreabundancia de información sobre un tema.[28] Esta entronca con otro concepto muy asociado a internet y a la sobrecarga informativa: «infoxicación», una sobrecarga con la que nos es difícil lidiar. La necesidad de novedades hace que cambiemos colectivamente de un tema a otro de forma más rápida. Esto puede afectar a la capacidad de evaluar la información que consumimos o a la calidad de la información, dada la imposibilidad para los periodistas de estar al tanto de todo. La ciencia constata lo que es obvio: la infoxicación está reduciendo la capacidad de atención global.[29]

MANIPULACIÓN, POPULISMO, IDENTIDAD

En la guerra de la (des)información en internet, los capitanes de la manipulación cuentan con verdaderas infraestructuras: granjas de troles, de clics y de «Me gusta» y fábricas de contenido engañoso y memes. Son instalaciones —normalmente ubicadas en países como Bangladés, China, India, Tailandia o Rusia—[30] cuyos trabajadores tienen la función de usar miles de móviles para simular opiniones positivas y visitas de usuarios reales, o desequilibrar el flujo real de publicación, comentarios e interacciones en sitios web y redes sociales. Encienden dispositivos a tropel y los ponen a ver vídeos, a hacer clics en las webs de quienes hayan pagado por ello o a difundir un contenido determinado con el fin de crear una tendencia, de acaparar la atención o de expulsar una tendencia anterior.

Algunas de esas granjas están dirigidas por experiodistas. El británico Peter Pomerantsev, experto en propaganda nacido en la URSS, visitó una de ellas en San Petersburgo, de vuelta a su país natal:

> Dentro de la granja, cada piso estaba lleno de ordenadores apiñados en estrechas filas y atendidos las veinticuatro horas del día; los empleados cambiaban de turno con pases que registraban todos los horarios de llegada y de salida. Incluso las pausas para fumar estaban reguladas.

> La granja tenía su propia jerarquía. Los más despreciados eran los «comentaristas», entre los cuales los de más bajo rango publicaban en las secciones de comentarios de los periódicos *online*; un nivel más arriba estaban los que dejaban comentarios en redes sociales. Los editores de mayor jerarquía instruirían a los comentaristas sobre qué figuras de la oposición rusa atacar, y pasarían sus días acusándolos de ser títeres, traidores, cómplices de la CIA. Algunos de los comentaristas no tenían una buena educación y su ruso escrito podría no ser muy bueno, por lo que un profesor de lengua acudía para darles lecciones de gramática.[31]

Así, cual organización militar, trabaja el ejército de la (des)información, y no es necesario visitar una de estas granjas para comprobarlo. Basta con observar lo que ocurre en redes sociales. Ben Nimmo, investigador de Oxford, demostró en 2019 cómo el tráfico de Twitter puede ser manipulado.[32] Distorsionar el flujo de contenido en redes sociales es, además, algo sencillo de hacer. Lo que importa no es tanto la calidad como la cantidad; dando a un pequeño grupo de usuarios la apariencia de un movimiento grande y creando tendencias falsamente genuinas y orgánicas, que parecen brotar de forma natural. Nimmo analizó el caso de los partidarios del político francés de extrema derecha Jean-Marie Le Pen, presidente del Frente Nacional, y cómo sus seguidores lograron en distintas campañas de 2017 que sus etiquetas (*hashtags*) fueran tendencia. Es solo un ejemplo entre muchos.

Todas estas herramientas y estrategias solo han amplificado lo que ya venía practicándose, como hemos comprobado, hace cientos, miles de años: el uso de estrategias de desinformación en la guerra política propagandística. Aunque no está claro el origen del término *per se*, la historia apunta a la Primera Guerra Mundial. Cuenta el espía soviético Walter Krivitsky[33] que el Estado Mayor alemán tenía un departamento conocido como Servicio de Desinformación. Dicho organismo se dedicaba a elaborar planes y órdenes militares secretos aparentemente plausibles que se aseguraban de que llegaran a manos del enemigo como documentos auténticos. Después, bajo el mandato de Stalin, el servicio secreto soviético (en el que Krivitsky sirvió) adoptaría en gran medida el término y las técnicas asociadas a él.

Pomerantsev cuenta cómo las estrategias de desinformación actuales se empezaron a aplicar en la Rusia de finales de los años noventa, coincidiendo (no por casualidad) con la campaña electoral que dio la presidencia a Vladímir Putin hasta hoy. El artífice de tales estrategias fue Gleb Pavlovski, un médico que había dirigido en 1996 la campaña del expresidente Borís Yeltsin. A Pavlovski se le considera el creador de la figura de Putin y de los principios del sistema político en la Rusia «putiniana».

Cuando Pavlovski investigaba cómo encauzar sus estrategias de campaña en los años noventa, descubrió que los rusos asumían contradicciones que no encajaban en las etiquetas tradicionales de «izquierda» o «derecha». La mayoría creía en un Estado fuerte, siempre que este no se inmiscuyera en sus vidas personales. Por eso experimentó con un enfoque diferente: no se centró en el argumento ideológico, sino en juntar grupos sociales distintos, a menudo en conflicto, cohesionados por una emoción central: un sentimiento lo suficientemente poderoso como para unirlos, pero

lo bastante vago como para significar cualquier cosa para cualquiera. Un cuento de hadas.

En las elecciones presidenciales de 2000, el cuento de hadas fue hacer creer a todos los que se habían quedado atrás en los años de Yeltsin que aquella era su última oportunidad para convertirse en ganadores. Eran segmentos dispares de la sociedad, agrupados bajo la idea de «la mayoría de Putin».

Tal vez esta historia les resulte familiar. Es la misma que contó el presidente estadounidense Donald Trump a su electorado dieciséis años después; la misma que creyeron los votantes del «sí» al Brexit en el Reino Unido. Es el populismo de una era postideológica en la que las viejas categorías sociales se han derrumbado, fruto de la cosmovisión que reemplazó a la ideología tras la Guerra Fría.[34] En ella no hay idea de historia ni del futuro. No es una batalla de valores, de la democracia contra el autoritarismo, sino una guerra de información.

Cuando las viejas concepciones de ideología o de clase se difuminan, la nueva estrategia se dirige a una cultura identitaria. El objetivo es encontrar grupos dispares y vincular el comportamiento de voto deseado con lo que más importe en ese momento. Dada la fragmentación social, el grupo identitario bajo el que reunirlos debe ser lo bastante amplio como para que una gran mayoría se proyecte en él. Conceptos generales como «el pueblo», «la gente» o «personas reales como tú», con un enemigo común abstracto como «las élites», «el sistema» o «el poder».

Se trata de ir un paso más allá en la ingeniería del consentimiento de la época de Edward Bernays. Esta se dirigía a grupos formales, algo que no resulta hoy suficiente por no representar unas claras categorías sociales. Hay que conectar con la gente en función de las causas que les mueven, ya sea el medio ambiente, los derechos de los animales, el derecho a la propiedad, el derecho o no al aborto, o el matrimonio gay. Todo ello con la idea de un mundo mejor, de volver a convertirse en ganadores, de tomar (de nuevo o por primera vez) el control.

POSVERDAD, IGNORANCIA, CONSPIRANOIA

En la lógica de las emociones, los hechos se convierten en algo secundario. No se trata de ganar un debate ideológico con argumentos. En un mundo dominado por la cosmovisión de la guerra de la (des)información, en el que la imparcialidad es imposible, los hechos ya no son sagrados. El futuro, entonces, deja de estar guiado por una visión basada en la evidencia. Al contrario, se le mira con el prisma del pasado, de la falsa promesa de lo que la intelectual Svetlana Boym definió como «nostalgia restauradora»: un esfuerzo por revivir un pasado deseado e idealizado que nunca existió y que, por tanto, no puede ser restaurado.

Seguimos anclados en la era de la posverdad, en la que los hechos objetivos influyen menos en la formación de la opinión pública que aquello que apela a la emoción y las creencias personales.[35] Un contexto en que el mundo percibido y el

real son cada vez más distantes; en el que la creencia, no los datos, dicta si algo es verdad o mentira. Y la creencia es muy difícil de cambiar, porque es una cuestión de fe.

Las creencias resultan, además, reforzadas por las dinámicas *online*. Desde hace unos años se habla de los «filtros burbuja». Son, según el creador del término, Eli Pariser, «el universo propio, personal y único de información que uno vive en la red».[36] Lo que haya dentro de este universo personal *online* depende de lo que uno es y lo que uno hace, pero uno no decide qué entra ni sabe qué se elimina. Son filtros que personalizan nuestra búsqueda en Google o que seleccionan lo que aparece en nuestro muro de Facebook, que, según Pariser, tratan de complacernos y tienden a la segregación.

Las personas son proclives a buscar certezas a través del contacto social, y este comportamiento *online* puede convertir sus redes en cámaras de eco. Con ello se reafirman y protegen del desacuerdo. Esta tendencia aumenta más en momentos de creciente incertidumbre, con una propensión a preferir la certeza, la estabilidad y la familiaridad frente a lo desconocido como potencial amenaza.

Si bien hay mucho de cierto en todo esto, no está claro el mecanismo de los filtros burbuja. De hecho, varios estudios sugieren que funcionan más bien al contrario de lo que sostiene Pariser: no es que los filtros *online* ofrezcan contenido menos diferente y por eso nos afiancemos más en nuestras propias creencias, sino que, al exponernos a una mayor diversidad de contenido más partidista en el sentido opuesto a nuestras opiniones, se refuerza y se polariza más nuestra visión.[37]

A este efecto potenciador en los entornos *online* se une la propagación del extremismo y de la manufactura de la ignorancia. La confluencia de la desinformación *online* y de unos viciados sistemas de recomendación han dado lugar a la nueva era de la «agnotología» de masas,[38] de cómo se fabrica estratégicamente la ignorancia mediante la perversión de las herramientas de producción de conocimiento.

Hay todo un engranaje funcionando para ello. Una de sus tácticas consiste en crear términos ex profeso. Por ejemplo, el Partido Republicano estadounidense acuñó en los años noventa términos como «impuesto a la muerte» (en lugar de impuesto de sucesiones) para asociar a él connotaciones negativas. Para lograr que permease, creó primero un mundo de contenido que acababa llegando a los medios de comunicación en el momento adecuado para que, cuando alguien buscase el término, obtuviera un resultado específico. Algo parecido sucedió con «cambio climático»: el término ya había sido creado, pero los republicanos forzaron su uso en lugar de «calentamiento global».

Como explica la académica Danah Boyd,[39] este tipo de técnica de manipulación explota la falta de información y contribuye a fraccionar el conocimiento y a generar dudas. Ese es precisamente el fin: lograr la fragmentación epistemológica, cómo sabemos lo que sabemos, o cómo accedemos al conocimiento.

La «luz de gas» es otra táctica frecuente. Es un tipo de manipulación que trata de provocar que otra persona (o grupo de personas) cuestione su propia realidad, memoria o percepciones. A menudo, el engaño consiste en tratar de convencer de la existencia de un hecho falso y de la no existencia de un suceso real. Si bien este procedimiento es un clásico entre dictadores, narcisistas, líderes de culto y abusadores, su uso se extiende a todo tipo de actores en el mundo *online*.

Este tipo de estrategia no es nueva ni propia de internet, pero este canal de distribución masiva facilita su propagación y potencia su efecto. Y basta con poco: sembrar la duda es suficiente. Asegurar que sea más fácil acceder al contenido dudoso y conspirativo que al científico. Lo siguiente es socavar la información científica disponible para que, de llegar hasta ella, pierda al menos en parte su credibilidad.

Un método para ello es explotar los vacíos de datos, áreas dentro de un ecosistema de búsqueda donde no hay datos relevantes. Otro es cooptar un término abandonado o desgastado y darle un nuevo significado. Por ejemplo, si buscamos en YouTube el concepto *social justice*, el primer resultado que aparece[40] ofrece una visión cuando menos torticera y manipulada del término. Es un vídeo de Prager University, o PragerU. Aunque se autodenomina *university*, se trata de una compañía audiovisual no acreditada como institución académica cuya misión es contrarrestar las, a su juicio, ideas izquierdistas que se enseñan en las universidades y que «arruinan todo lo que tocan».[41]

El vídeo está bien producido, contiene muchos de los principios de la alfabetización mediática y plantea cuestiones difíciles para hacerlo creíble. Sin embargo, en realidad ofrece una visión parcial y ligeramente conspirativa de lo que es la justicia social. El propósito es, en realidad, denostar este término y reprimir su uso.

Si seguimos viendo vídeos, en un momento dado llega el activismo de los guerreros de la justicia social, antifeministas y homófobos. Lo mismo sucede al buscar vídeos de salud: aunque acudas a la página de una organización con autoridad y científicamente respaldada, casi siempre aparecerá en la rueda de recomendación un vídeo «conspiranoico», ya sea antivacunas o promotor de cualquier seudociencia. ¿Por qué? Porque quienes están detrás saben cómo generar esas conexiones.

La asociación que hace que de un contenido «seguro» se llegue a otro desinformativo o falso se puede producir de otras maneras, a veces incluso de forma involuntaria. A menudo son los medios los que lo propician, al tratar de mostrar dos visiones contrapuestas —por ejemplo, provacunas y antivacunas— en un empeño erróneo por crear debate a partir de una falsa equivalencia. Conceder un espacio a personas que promueven información falsa y que toman posturas extremas envía una señal a YouTube de que ese contenido es relevante y será enlazado en las búsquedas de información, en este caso sobre vacunas.

De este modo, una persona que visita YouTube para obtener información razonablemente fundamentada está expuesta a contenido marginal, extremista o

conspirativo. Sus creadores afirman proporcionar una fuente alternativa de información. Es lo que la investigadora Rebecca Lewis denomina «influencia alternativa».

Así, una teoría de la conspiración que empieza como una publicación en redes sociales puede llegar a las masas. QAnon es un ejemplo de cómo un fenómeno marginal puede convertirse en un movimiento. Se trata de una teoría conspirativa según la cual el mundo está dirigido por una cuadrilla de demócratas pedófilos adoradores de Satanás que intrigan contra Trump mientras operan en una red mundial de tráfico sexual de niños.[42] De acuerdo con QAnon, Trump es el mesías destinado a romper esta conspiración criminal y llevar a sus miembros ante la justicia. El expresidente estadounidense, que sale obviamente beneficiado con esta teoría, no solo no ha renegado de ella, sino que ha reconocido su existencia y ha alabado su supuesta (y falsa) lucha contra la pedofilia.[43]

Los millones de seguidores en Facebook de QAnon han traspasado las fronteras de internet con su discurso del odio. En su nombre se han cometido delitos y crímenes, y la teoría y sus seguidores han sido calificados como una potencial amenaza terrorista nacional en Estados Unidos. Incluso entraron en las filas políticas, de la mano de la excongresista Marjorie Taylor Greene. La «conspiranoia» llegó hasta Japón, Brasil o la extrema derecha alemana. Su siguiente paso es alcanzar un público más amplio: antivacunas, creyentes en alienígenas y ciudadanos comunes que cuestionan la amenaza de la pandemia.

Así se facilita la banalización ideológica, la ausencia de empatía, la radicalización y la microsegmentación política *online*. No hay debate ni enfrentamiento de ideas o valores, más allá de los choques de opiniones partidistas. El propio Trump fue durante su presidencia un vector *online* del discurso de odio, con consecuencias sangrientas. Entre ellas, el asalto al Capitolio de Estados Unidos más violento hasta la fecha, a raíz de la negativa del expresidente a aceptar su derrota electoral y la victoria de Joe Biden en las elecciones de noviembre de 2020.

Ello llevó a una parte del electorado de Trump a irrumpir por la fuerza en el Congreso estadounidense el 6 de enero de 2021. El suceso se saldó con cinco personas muertas, al menos 81 miembros de las fuerzas de seguridad del Capitolio y 65 policías heridos, así como dos suicidios posteriores de oficiales.[44] Se arrestó a 440 acusados, y la cifra de detenidos a fecha de abril de 2021 seguía creciendo.[45]

También hubo consecuencias *online* inauditas: Twitter y Facebook expulsaron a Trump de sus plataformas. De forma paralela, Apple y Google bloquearon la *app* de la red social Parler, que había atraído a los seguidores del expresidente estadounidense. Amazon también dejó de alojar en sus servidores el contenido de Parler, dada la escalada de contenido violento.

SOCAVAR LA DEMOCRACIA

En este contexto, la desinformación, el odio y la retórica polarizante —que impregnan un ecosistema mediático en el que cualquiera puede creer cualquier cosa — han empezado ya a minar la democracia. La información es un elemento fundamental para la formación de la opinión pública. Si lo que impera es lo contrario (la desinformación) o una sobreabundancia de contenido que conduce a informarse mal, si las vulnerabilidades de la arquitectura de las principales plataformas *online* y de las redes sociales permiten a quien se lo proponga modelar el conocimiento público de manera profunda, estamos perdidos.

La apertura de internet y de las diversas plataformas de publicación de contenidos —incluidos blogs y redes sociales— desintermedió la comunicación, dio voz y acceso directo a las fuentes y empoderó a los usuarios no solo en el descubrimiento de contenido, sino también en la difusión y distribución de testimonios, comentarios o noticias fuera de los canales de información tradicionales. También abrió un nuevo espacio para la esfera pública: convirtió a estas plataformas en la nueva «plaza del pueblo», una infraestructura clave para el discurso público y político.**[46]**

Sin embargo, en esta nueva plaza del pueblo vale todo. Se cuelan textos, audios y vídeos con aspecto informativo (estructura de titular, subtítulo y cuerpo de texto; personas que simulan ser presentadores en un estudio de televisión, etc.) que son en realidad falsos. Se legitima así un contenido que, además, llega hasta las redes personales de los usuarios; una doble legitimación a base, únicamente, de popularidad.

Esto está afectando a la comprensión de la realidad por parte de la ciudadanía y está socavando la confianza, el diálogo informado, un sentido compartido de la realidad, el consentimiento mutuo y la participación.**[47]** Además, se dificulta el cuestionamiento de lo que dicen líderes políticos y empresariales, gobiernos y otras instituciones que evitan el escrutinio al dirigirse a la gente directamente a través de internet. Esto requiere que las plataformas *online* cumplan un rol de guardabarreras, como lo son los periodistas y los medios de comunicación, con sus consiguientes controles y responsabilidades, entre otras, de verificación. Es un papel que se niegan a aceptar o que —como veremos más adelante en este libro— ejercen muy tímidamente.

Los medios de comunicación tradicionales tienen obligaciones informativas y deben rendir cuentas por su trabajo, algo que no es así ni para Google, ni para Facebook, ni para YouTube, ni para ninguna red social. Al menos no de momento. A diferencia de los medios, estas no tienen responsabilidad legal sobre el contenido que se vierte en ellas. Además, las plataformas cuentan con una clara ventaja a la hora de hacer frente a las ansias de inmediatez de los usuarios: el contenido se comparte en tiempo real, mientras que las noticias requieren un tiempo de elaboración que permita contrastar los hechos.

Mientras las plataformas se lucran con la publicidad *online*, los medios ven mermados sus ingresos, las condiciones de los periodistas se precarizan y la profesión

pierde confianza y respeto. Lo hace, paradójicamente, en el momento en el que más necesaria es su función de servicio público para satisfacer el derecho a una información verificada y contrastada frente a la avalancha de desinformación.

A ello se suma la escasa alfabetización social en capacidades de verificación, lo que se traduce en una mala preparación para determinar la autenticidad de una noticia.[48] Así sigue su curso el contenido diseñado para confundir y minar la confianza en las instituciones democráticas, desde el sistema electoral hasta el periodismo. Son elementos comunicativos engañosos disfrazados de reales, fáciles de confundir para quienes no tienen herramientas para distinguir una cosa de la otra.

El riesgo es mayor, como de costumbre, para los más vulnerables, quienes menos recursos tienen. ¿Qué sucede si tu única fuente de información es Facebook o WhatsApp? Como comentábamos anteriormente, en países como Birmania, Facebook es internet. Es la principal fuente de noticias para dos de cada cinco usuarios birmanos.[49] Allí «conectarse» se dice en jerga «line paw tat tal», que viene a ser también «activo en Facebook».[50] La desinformación *online* es gratuita (siempre y cuando algún poderoso no decida apagar internet), pero no todo el mundo tiene acceso a periodismo de calidad o a medios comunicación independientes, o, aunque lo tenga, tal vez no sepa cuáles son estos.

Todo esto sucede en un momento en el que somos más vulnerables. El extraordinario crecimiento económico y las mejoras generalizadas en el bienestar observadas durante las últimas décadas no han logrado cerrar las profundas divisiones entre países y dentro de ellos.[51] Vivimos mejor, tenemos mayor calidad de vida, pero la desigualdad entre diferentes grupos de la población aumenta. Hoy el mundo es más rico, pero también más desigual que nunca.[52]

Esto indudablemente crea fricciones. La fragmentación social y la desigualdad entre los grupos son aprovechadas por los estrategas de la propaganda y la desinformación para agotar la verdad. La microsegmentación surte efecto y contribuye, a su vez, a reforzar la fractura social. La falta de consenso sobre la verdad, incluso dentro de las propias fronteras, es aprovechada para manipular, lo que a su vez consolida la posverdad en un expansivo efecto espiral.

La desigualdad se manifiesta también en lo peor del ciberespacio como consecuencia de codificar programas informáticos y trasladar a internet el odio, la violencia, la infelicidad y la visceralidad humanos. En este capítulo hemos visto muchos ejemplos de ello. En el siguiente nos adentraremos en las tecnologías que refuerzan dichas desigualdades y los sesgos asociados a ellas, que criminalizan a personas de color, que discriminan a las mujeres, que automatizan y precarizan el trabajo, que reducen las oportunidades para personas con capacidades diferentes[*], que excluyen a personas vulnerables de coberturas sociales y de salud, que sistematizan el extremismo y el odio… Tecnologías, en fin, que reproducen lo peor del ser humano[**].

6

Discriminación

Las aplicaciones matemáticas que alimentan la economía de datos se basan en elecciones hechas por seres humanos falibles. […] programan los prejuicios, malentendidos y sesgos humanos en unos sistemas informáticos que administran cada vez más nuestras vidas. Como dioses, estos modelos matemáticos son opacos, y su funcionamiento es invisible para todos, excepto para los sumos sacerdotes de su dominio: matemáticos e informáticos. Sus veredictos, incluso cuando son incorrectos o perjudiciales, están fuera de discusión o apelación. Y tienden a castigar a los pobres y oprimidos en nuestra sociedad, mientras enriquecen a los ricos.

CATHY O'NEIL,
Armas de destrucción matemática

¿Cómo se supone que debes reaccionar cuando un algoritmo te llama *gook*? La pregunta retumbaba en la cabeza de la periodista Julia Carrie Wong. Ella solo pretendía divertirse cuando introdujo su foto en una aparentemente inofensiva aplicación que se había vuelto viral a base de ofrecer descripciones de las personas a partir de imágenes de sus caras. Desde luego, no esperaba recibir una respuesta tan insultante.[1] *Gook* es un término despectivo usado por el ejército de Estados Unidos durante las guerras de Corea y de Vietnam para referirse a personas de ascendencia asiática. Y ahora esa dichosa máquina le había llamado así a ella.

Su colega de profesión Stephen Bush no corrió mejor suerte. La *app* le llamó *blackamoor*, una palabra usada para referirse a los esclavos o sirvientes negros. Y también «negroide», y de ahí pasó a «malhechor, delincuente, convicto».[2] Teniendo en cuenta que la biblioteca de imágenes usada por la aplicación es una de las más nutridas de la historia de la inteligencia artificial (IA),[3] desarrollada por las universidades de Stanford y Princeton (Estados Unidos), da que pensar. Entre otras cosas porque en esa misma colección se basan numerosos algoritmos de identificación de imágenes en funcionamiento.

La anécdota ilustra lo que hoy es una realidad extendida ahí fuera: vivimos en un mundo *online* donde algoritmos informáticos con problemas intrínsecos de clasificación y sesgos gobiernan el acceso y exclusión a la información y a las oportunidades, juzgan y toman decisiones de forma arbitraria.

Los algoritmos son los códigos matemáticos que rigen el funcionamiento de Google, Facebook, Amazon, YouTube y toda clase de plataformas y aplicaciones. Son secuencias de pasos que no ejecuta una persona, sino una máquina. Son el

corazón de los sistemas informáticos y de la inteligencia artificial. Como ya hemos visto en capítulos anteriores, la IA son sistemas informáticos avanzados que intentan funcionar como el cerebro para procesar información de forma compleja, aprender, detectar patrones, hacer recomendaciones y asistir en la toma de decisiones. Gracias a internet, al llamado «big data» (macrodatos) y al desarrollo de ordenadores más rápidos, es posible aprovechar este tipo de técnicas que estaban disponibles antes, pero que no eran tan avanzadas como lo son en la actualidad.

El nacimiento de internet propició la generación masiva de datos y la generalización de los sistemas de almacenamiento y gestión de la información. El volumen de los datos existentes es de tal magnitud que, si ocupara un espacio físico, superaría el tamaño de una galaxia. Esto ha propiciado la inteligencia de datos del big data y, con ella, el desarrollo de la IA.

La IA está hoy por todas partes, omnipresente en la red. Selecciona la música que escuchamos *online*, nos sugiere qué series ver en cualquiera de los múltiples servicios de entretenimiento bajo demanda, condiciona qué leemos cuando navegamos por el ciberespacio o las *apps* móviles, o guía nuestros movimientos mediante instrucciones GPS. Responde a cada búsqueda en internet, a nuestras órdenes a los asistentes virtuales que acompañan a los dispositivos conectados. Se ha metido en nuestros bolsillos, hogares y vehículos. Puede ver, leer, escuchar y dar respuesta. Lo mismo limpia el suelo que redacta noticias, traduce textos, recomienda estrategias de negocio o una buena dieta, analiza nuestra salud o asiste en la conducción y en tantas otras tareas.

Estos sistemas aprenden de nosotros para mejorarse a sí mismos. Para eso y para servir mejor a quienes los controlan: los gigantes tecnológicos y las terceras partes que usan nuestros datos personales para lucrarse de formas infinitas. Por ejemplo, creando programas informáticos basados en esos datos que automatizan procesos de selección de personal, de concesión de créditos o de primas de seguros, de asignación de recursos y un largo etcétera.

Dichos sistemas, lejos de ser perfectos, asumen los sesgos y prejuicios humanos presentes en el lenguaje del que aprenden.[4] Automatizan las desigualdades y perpetúan la discriminación[*] por raza, género, religión, ingresos, capacidades o tendencia sexual. Crean ciclos de retroalimentación que eternizan la injusticia. Y, dado que se están utilizando para tomar decisiones importantes en muchos sectores, tienen un poder creciente sobre la acción humana, incluso por encima de ella: se objetivizan con la supuesta imparcialidad de los números y se presentan como verdades absolutas.

Bajo dicha apariencia se esconde la realidad de unos sistemas que, lejos de operar sin prejuicios, están diseñados y desarrollados por humanos que introducen sus sesgos y su ideología en ellos. Son, dice la matemática Cathy O’Neil, «armas de destrucción matemática»[5] opacas y defectuosas. Con la promesa de eficiencia y justicia, exacerban la realidad y castigan a los pobres.

Son los sistemas algorítmicos de toma de decisiones[6] (ADM) y llevan muchos años en nuestras vidas. Hay constancia de discriminación algorítmica ya en los años ochenta.[7] Su versión modernizada son las herramientas digitales basadas en «big data» e IA, pero aún siguen usándose programas de este tipo más antiguos y básicos e igual de dañinos. Su perfeccionamiento reciente condujo a un *boom* allá por 2010, cuando proliferaban hasta debajo de las piedras. Empezaban a operar en todos los sectores imaginables, a tomar decisiones sobre solicitudes de empleo o universitarias, préstamos bancarios, concesión de ayudas o acceso a los servicios de salud.

Hay centenares de casos conocidos sobre cómo discriminan estos sistemas: en educación, trabajo, vivienda, salud, servicios sociales, justicia o información; por razones de raza, género, religión, tendencia sexual, ingresos o capacidad; negando recursos u oportunidades, invisibilizando, esclavizando. En su libro *Armas de destrucción matemática. Cómo el big data aumenta la desigualdad y amenaza la democracia*, O'Neil lo ejemplifica con multitud de casos reales. También lo hace Virginia Eubanks en *La automatización de la desigualdad. Herramientas de tecnología avanzada para supervisar y castigar a los pobres*.[8] Muchos otros ejemplos los hemos conocido gracias a investigaciones periodísticas.

INJUSTICIA POR SISTEMA

Un caso muy sonado fue el de COMPAS, una herramienta de análisis de riesgo delictivo basada en IA que aprende de todas las sentencias dictadas anteriormente. Su función es evaluar la probabilidad de que un delincuente acusado reincida. Un análisis de *ProPublica*[9] demostró en 2016 que a los acusados negros se les asignaba con mucha mayor propensión un riesgo de reincidencia alto, mientras que a los acusados blancos, erróneamente, se les atribuía con mayor frecuencia un bajo riesgo de reincidencia. Es decir, el sistema discriminaba a las personas de color. No funcionaba correctamente ni resolvía nada que no hubiera problematizado en primer lugar, dado que el sesgo racial es matemáticamente inevitable.[10]

Otra investigación periodística condujo a la conclusión de que los vecindarios poblados por minorías de color pagan primas más altas por los seguros de sus coches que los barrios blancos con el mismo riesgo: hasta un 30 por ciento más que en otras áreas con similares costes por accidentes.[11]

También sucede lo contrario. *ProPublica* demostró cómo la personalización *online* discrimina a los perfiles con mayores ingresos, para quienes se fijan precios más altos.[12] Diferentes personas acceden a una misma web, pero con resultados diferentes: por ejemplo, el buscador de viajes Orbitz mostraba hoteles de mayor precio a los propietarios de ordenadores Mac, mientras que la proveedora de mobiliario de oficina Staples ofrecía en su web sus productos a diferentes precios según el código postal del usuario en cuestión. Segregación geográfica y por nivel de renta en toda regla.

En 2016 se descubrieron casos de discriminación en la publicidad dentro de Facebook: anuncios de empleo que excluían a mujeres y a personas mayores en edad de trabajar, o anuncios de vivienda que excluían a negros e hispanos.[13] A pesar de las promesas de la red social de arreglarlo, en 2019 el algoritmo encargado seguía sesgando a la audiencia en función del contenido del propio anuncio.[14][15] Como resultado, incluso cuando los anunciantes intentaban llegar a un público diverso, no siempre podían hacerlo.

El caso de Facebook no es anecdótico. La selección de talento es uno de los campos donde se hacen más patentes los defectos de los programas destinados a automatizar el proceso o a hacerlo más eficiente. Programas que escanean millones de sitios web de empleo y analizan los datos sociales de cada persona para proponer a los mejores candidatos, con una visión a menudo distorsionada y que obvia que la vida *offline* de las personas no se refleja enteramente en internet.

Además, estos programas a menudo basan su configuración del candidato ideal en función de las personas que históricamente han ocupado ese tipo de puesto, lo cual se ha demostrado que lleva a un marcado sesgo contra las mujeres (privadas durante siglos de acceso a puestos de poder y a multitud de trabajos) y contra ciertas minorías. Hay muchos casos reales de mujeres afectadas por sesgos en procesos algorítmicos de búsqueda de trabajo. Uno de ellos es el de Esther Sánchez, que paradójicamente es especialista en recursos humanos:

> Durante el primer mes de búsqueda de empleo, en mi perfil de LinkedIn decía que era «directora de Personas/directora de RRHH». A raíz de una conversación con un cazatalentos, descubrí que si pones el título profesional en femenino el motor de búsqueda no te enlaza, por lo que ningún reclutador te encuentra. Hicimos la prueba en el curso de la conversación y me quedé atónita. Fue cambiar y poner «HR Director» y de repente le aparecí [en su pantalla].
> Por otra parte, en ninguna solicitud de trabajo *online* sabes cuáles son los filtros de los sistemas ADM que hay detrás y que te pueden descartar por la fecha de tus titulaciones. En algunas ofertas has de especificar no solo el código postal, sino también la dirección y la localidad. Es una caja negra que da paso a cualquier tipo de sesgo, pensamiento excluyente o puras especulaciones, que acaban derivando en exclusiones.
> Esta falta de información se ve reforzada por *e-mails* de desestimación de candidaturas automatizados, que no acostumbran a ir firmados por personas físicas y que nunca incluyen una explicación de por qué te han excluido del proceso. Esto sería útil tanto para disponer de información objetiva con la que descartar cualquier indicio discriminatorio como para proporcionar un retorno útil que le sirva [a la candidata o candidato] para posteriores ofertas.[16]

La experta comenta también las dificultades añadidas para personas que no tengan muchas destrezas digitales, dado que los numerosos requisitos de cumplimentación en procedimientos de selección automatizados «son desgastantes y disuasorios».

Hay más formas en que estos procesos discriminan a personas con capacidades diferentes. Las herramientas de videoentrevista automatizadas en tiempo real —como HireVue— pueden convertirse en una pesadilla. Así fue para Jessica Clements, una candidata cuya discapacidad visual le supuso una desventaja a la hora de enfrentarse a este sistema: no podía leer bien las preguntas y la luz de la cámara la cegaba.[17]

El sector de la vivienda es otro claro ejemplo de discriminación, y no solo mediante anuncios microsegmentados en redes sociales. Hablamos de algo más grave: los sistemas de calificación electrónica. Usan datos de patrones *online* de navegación y compra, e incluso la localización del usuario, con objetivos múltiples. Por ejemplo, para evaluar la idoneidad de un individuo como blanco de venta de una tarjeta de crédito o de un crédito rápido que necesita, pero por los que, debido a su condición vulnerable, pagará un alto interés.[18]

Este tipo de sistemas se está usando también para decidir puntajes de riesgo crediticio sobre alquileres, seguros de salud o hipotecas. El exvicepresidente de Google Douglas Merrill vio claro su potencial y fundó en 2009 Zest AI, un sistema de IA para bancos y cooperativas de crédito que escarba en internet para encontrar todo tipo de datos de los potenciales prestatarios. Dice ir «más allá de las limitaciones estadísticas y de datos de las puntuaciones crediticias tradicionales». Lo que se olvida de mencionar es que, mientras estas están reguladas, su sistema no lo está.

Facebook ha hecho también una incursión en este mercado con un sistema de puntaje crediticio basado en la calificación media de los amigos del usuario solicitante en la red social. La patente de dicho invento habla de su posible uso por parte de prestamistas. Dice así:

> Cuando un individuo solicita un préstamo, el prestamista examina las calificaciones crediticias de los miembros de la red social del individuo que están conectados con él a través de nodos autorizados. Si la media de la calificación crediticia de estos miembros es al menos una calificación crediticia mínima, el prestamista continúa procesando la solicitud de préstamo. De lo contrario, se rechaza la solicitud.[19]

Esto significa que un banco o un arrendador podría rechazar una solicitud de crédito o de alquiler si las personas con las que el solicitante está conectado en Facebook tienen un mal historial crediticio. Que el individuo en cuestión tenga suficiente solvencia poco importa. ¿Justicia, dicen? Que se la pidan a otros.

Otro polémico ámbito de aplicación de estos algoritmos es el de la salud y la asignación de recursos. En 2016, Arkansas (Estados Unidos) recurrió a un ADM para gestionar las ayudas de salud de un programa estatal de discapacidad. El programa decidía si los solicitantes tenían derecho a recibir un cuidador personal en sus casas y durante cuántas horas. Algo que antes realizaba una enfermera tras visitar a cada paciente lo hacía entonces esa nueva herramienta sobre la base de una encuesta a los potenciales beneficiarios. Como consecuencia, muchas de esas personas vieron reducidas drásticamente las horas de asistencia asignadas, y —¡sorpresa!— resultó ser por un error de la máquina.[20] Dadas las pocas posibilidades de los afectados de impugnar las decisiones del algoritmo, decidieron demandar al sistema, y ganaron.

Este caso tampoco es único. No solo se han conocido más desde entonces, sino que probablemente hay otros muchos que se desconocen, dado el extendido uso de los sistemas de asignación algorítmicos. Si en el ejemplo anterior los perjudicados eran personas con alguna discapacidad, en muchos otros lo son personas de color. En

2019, un grupo de investigadores descubrió que un algoritmo ampliamente utilizado por los profesionales de la salud en Estados Unidos estaba dejando fuera a más de la mitad de los pacientes negros que necesitaban atención sanitaria adicional.[21] El motivo: el algoritmo utilizaba el historial de costes de salud como indicador de las necesidades de salud, pero no tenía en cuenta que, por razones discriminatorias o de pobreza, históricamente se había gastado menos dinero en pacientes de color con un mismo nivel de necesidad.

Un caso más reciente que ha generado controversia es el ADM usado en Estados Unidos para decidir quién puede acceder a una vacuna contra la COVID-19. Es un sistema automatizado que desde los comienzos fue criticado por la falta de transparencia sobre las fórmulas de priorización, que no son homogéneas y que agravan las disparidades en el acceso a las vacunas.[22] Eso, además de crear más caos y complicaciones burocráticas, según los profesionales sanitarios.

A la lista de algoritmos de toma de decisiones fallidos se suman varios en el Reino Unido. El Gobierno se ha visto obligado a retirar un sistema policial para predecir delitos con tasas de error de entre el 49 por ciento (en los mejores escenarios) y el 82 por ciento. El sistema, en el que el Gobierno invirtió diez millones de libras (algo más de once millones de euros), era potencialmente discriminatorio.[23] También ha retirado un programa de asistencia a la asignación de visados —usado durante años— por acusaciones de racismo arraigado.[24]

Sin embargo, el sistema cuya cancelación en el Reino Unido tal vez haya sido más polémica es el algoritmo que el Gobierno usó como sustituto de los exámenes de acceso a la universidad en 2020. Debido a la pandemia de la COVID-19, estas pruebas no se pudieron realizar y, como sustituto, se usó un programa que redujo las calificaciones del 40 por ciento de los estudiantes. Esta reducción afectó particularmente a aquellos que provenían de las zonas más pobres, que vieron truncados sus sueños de ir a las universidades que querían. Entre ellos, una joven que había ganado un premio literario en honor a Orwell con un relato casi premonitorio: trataba sobre un algoritmo que decide las calificaciones escolares según la clase social de los estudiantes.[25] Ver para creer.

La adopción agresiva de este tipo de algoritmos por parte del Reino Unido muestra los errores de tratar de automatizar el Gobierno con sistemas que no se han probado lo suficiente, y cuya eficacia —y no discriminación—, no ha sido demostrada con todos los grupos de población; sistemas cuya necesidad no se ha cuestionado. A pesar de ello, otros países en procesos similares caerán —o han caído ya— en la misma trampa. Algunos, como China, van un nivel más allá, como veremos en el siguiente capítulo.

España tampoco se libra, a pesar de no ser tan transparente con respecto a dónde y para qué se utilizan ADM. Herramientas como VeriPol, que sirve para ayudar a la policía a identificar denuncias falsas, han sido criticadas por su potencial para discriminar a inmigrantes, dado que su uso diferente de la lengua puede hacer creer al

sistema que mienten.[26] Los creadores de VeriPol aseguran que su criatura tiene una tasa de aciertos del 91 por ciento,[27] lo que significa que un 9 por ciento de los denunciantes (nueve de cada cien) son falsamente acusados de mentir.

Por otra parte, están los sistemas automatizados para calcular las prestaciones por desempleo. Durante los últimos ocho años han reducido en más de un 50 por ciento dichas ayudas, como informa AlgorithmWatch.[28] No está claro si dicha disminución es fruto de un defecto en los programas o se debe al uso simultáneo de sistemas incompatibles.

Luego hay otros sistemas que no se deben perder de vista. Por ejemplo, el e-Riscanvi, usado en Cataluña para evaluar el riesgo de reincidencia violenta de los presos. Recordemos que su análogo estadounidense —el sistema COMPAS— resultó tener un sesgo contra los presos negros, a quienes se les asignaba sin justificación un riesgo de reincidencia mayor.

También se usan en España sistemas algorítmicos para evaluar el riesgo de violencia en adolescentes (que en Estados Unidos han demostrado que discriminan de forma no intencionada), para predecir la necesidad de ayudas sociales para personas mayores, para predecir el riesgo futuro de conductas delictivas, para localizar mensajes de odio en redes sociales, para detectar el fraude de forma automática o para automatizar el diagnóstico médico.[29]

Si bien no todos estos sistemas están conectados o extraen datos *online*, tienden cada vez más a estarlo, dada la masa de datos personales que es posible interceptar en la red. Además, son una cómoda alternativa a otros sistemas como el bancario, estrictamente regulado. ¿Qué implicaciones tiene esto para el ciudadano de a pie? Lo explica bien O’Neil:

> Con el imparable crecimiento de las calificaciones electrónicas, nos asignan a lotes y categorías aplicando fórmulas secretas, algunas de ellas alimentadas por expedientes cargados de errores. No nos ven como individuos, sino como miembros de tribus y, una vez clasificados, no hay manera de deshacerse de la etiqueta.

TIERRA, TRÁGAME

Un caso mucho más banal que los anteriores, pero mucho más conocido, es el de los gorilas de Google. El sistema de reconocimiento facial de Google Photos etiquetó por error a la programadora Jackie Alcine y a un amigo (ambos afroamericanos) como gorilas. Aquello sucedió en 2015. Desde entonces se han multiplicado los incidentes de este tipo.

Muy sonados fueron los hallazgos de racismo en el sistema de recorte de imágenes de Twitter, que se enfocaba automáticamente en las caras blancas sobre las negras. La red social reconoció el error del algoritmo que automatizaba esta tarea.

¿Más ejemplos? En mayo de 2020 *The Guardian* reveló que Microsoft estaba despidiendo a periodistas y editores y reemplazándolos por un sistema algorítmico.[30] Este estaba diseñado para automatizar la labor de seleccionar las noticias que

aparecen en los portales MSN y Microsoft News. Poco después, dicho programa —basado en una técnica de IA llamada «aprendizaje automático»— metió la pata hasta el corvejón. El sistema ilustró una noticia sobre racismo que incluía reflexiones de la cantante mestiza Jade Thirlwall con una foto de su compañera de banda, la también mestiza Leigh-Anne Pinnock.[31] Paradójicamente, dicha selección reflejó el propio sesgo racial del sistema, incapaz de reconocer a dos personas por el hecho de ser mestizas.

La cosa no quedó ahí: Microsoft anticipó que su *software* seleccionaría artículos críticos sobre el anterior suceso y los publicaría automáticamente en MSN y otros portales. Ante su incapacidad para pararlo, ordenó eliminar tales noticias a quienes supervisaban dicho sistema (los periodistas y editores que aún no habían sido despedidos). He aquí un maravilloso y horrendo ejemplo del sinsentido del uso de tecnologías que no funcionan —y que ni siquiera sus creadores saben cómo lo hacen ni cómo pararlas— para automatizarlo todo. Y, de paso, perpetúan los sesgos humanos y la discriminación.

El traductor de Google —Google Translate— también usa en ocasiones lenguaje sexista en sus traducciones, a pesar de sus intentos por solucionarlo. Un simple experimento de AlgorithmWatch[32] mostró que Google cambiaba el género de algunas palabras «de una manera tremendamente estereotipada». «La presidenta» y «el enfermero», en alemán, se convierten en «el presidente», en italiano, y «la enfermera», en francés, respectivamente. En 2021, la matemática Clara Grima bromeó en Twitter sobre el hecho de que asociado a su nombre en el buscador pusiera «Matemático», en masculino.

Los asistentes virtuales de los móviles inteligentes y aparatos de todo tipo tampoco se libran. «Me sonrojaría si pudiera» es lo que respondía Siri al llamarle «zorra» (ahora su contestación ha cambiado por un «no responderé a eso»). Hasta la Unesco los ha calificado de sexistas. Una investigación conducida por este organismo mostró que la mayoría de los programas orientados a servicios (encender la luz, poner música…) usan una voz de mujer.[33] En cambio, cuando se trata de guiar o proporcionar instrucciones, se recurre a voces masculinas. «Esto no lo define la preferencia del consumidor, es la forma en que reproducimos una determinada comprensión del mundo: las mujeres son más cuidadoras y los hombres son quienes toman las decisiones», me comentaba al respecto la directora de la División para la Igualdad de Género de la Unesco, Saniye Gülser Corat.[34]

En realidad, Siri tiene voz de hombre por defecto en cuatro lenguas: inglés británico, neerlandés, francés y árabe. La Unesco lo achaca a que son países donde tradicionalmente ha habido sirvientes masculinos —mayordomos— en las clases sociales más altas.

Los filtros de mensajes no deseados o *spam* se suman también a la lista de los sesgos. Un experimento[35] ha revelado que Microsoft Outlook marca los mensajes como *spam* basándose en una sola palabra, como «Nigeria» o «sexo». De este modo,

se bloquean mensajes de forma discriminatoria, como puede ser una solicitud de beca universitaria de un estudiante nigeriano o información sobre un programa de educación sexual. Es una muestra más del racismo y los sesgos incrustados en el *software*.

La lista es larga y podríamos seguir con los ejemplos hasta escribir otro libro y unos cuantos tomos con ellos.[36] Las implicaciones sociales, cívicas y legales de los ADM discriminatorios son enormes y presentan amenazas significativas para nuestra sociedad. Nadie escapa. Nadie está a salvo de ellos. Aunque tiendan a penalizar a los colectivos más vulnerables, también castigan a los ricos.

PELIGROSAMENTE ESTÚPIDA

¿Por qué sucede todo esto? Hay varios factores en juego. Para empezar, la IA no es tan inteligente y su realidad es más trivial de lo que pueda parecer. Por ello, se considera técnicamente que la IA actual es «limitada» o «débil». Es capaz de resolver muy bien una única tarea una vez contextualizada. Sin embargo, es incapaz de sumar aprendizajes como las personas; un sistema de IA puede saber jugar muy bien al ajedrez, pero ser incapaz de encontrar un tumor en una imagen. Y, si aprende a identificar tumores, se olvidará de cómo jugar al ajedrez. Es lo que se conoce como «olvido catastrófico».

La IA es muy eficiente para procesar grandes volúmenes de datos y extraer patrones de ellos. Sin embargo, no sabe si esos datos están incompletos o si son buenos o malos, ni sabe cómo pensar en ello. No solo no entiende la información en los términos en los que lo haría una persona, sino que tampoco sabe contextualizarla ni establecer relaciones de causalidad. Puede apreciar que algunos eventos están asociados con otros eventos, pero no determinar qué cosas hacen que otras cosas sucedan directamente.

Comprender la causa y el efecto es un gran aspecto de lo que llamamos «sentido común», que es algo que la IA no tiene. Los sistemas más avanzados son capaces de simular un aparente sentido común, pero son simplemente eso: una simulación; adivinan mejor qué deberían responder a una determinada acción o requerimiento. Es lo que Dennett[37] denomina «competencia sin comprensión»: a escala funcional, un sistema puede alcanzar una cota de rendimiento (competencia) que en contextos humanos se atribuiría a la comprensión (es decir, la inteligencia), pero sin comprenderlo.

Por otra parte, las máquinas son capaces de hacer cosas que pensamos que son difíciles, pero son incapaces de aprender como los humanos habilidades psicomotrices o perceptivas que hasta un bebé tiene. Es lo que se conoce como «paradoja de Moravec».

Mientras escribo estas líneas leo en la prensa titulares como «Una IA arruina un partido de fútbol al confundir el balón de juego con la calva del árbitro». Suena casi a

chiste, pero es real: un claro ejemplo de la estupidez de estos sistemas. Igual confunden pelotas con calvas que chihuahuas con magdalenas, o a dos personas mestizas.

A veces esas confusiones tienen consecuencias mortales. En 2018, un coche autónomo de Uber atropelló a una mujer de Arizona (Estados Unidos). ¿El motivo? El sistema de IA que usaba el vehículo no tenía la capacidad de clasificar a un objeto como peatón si este no se encontraba cerca de un paso de peatones.[38] Es decir, el coche no reconoció que ese objeto que tenía delante era una persona que estaba cruzando la calle de forma imprudente. La mujer montaba en su bicicleta, y el coche alternó entre clasificarla como vehículo, bicicleta u objeto desconocido. En ningún caso previó la colisión: si era un vehículo o una bici, viajaría en la misma dirección que el coche de Uber, pero en el carril contiguo, y, si era un objeto desconocido, estaría estático. Cada vez que el sistema recalculaba la clasificación, lo trataba como un objeto nuevo, por lo que era incapaz de trazar su trayectoria anterior y calcular el probable choque.

Este tipo de errores —aunque por fortuna no siempre con consecuencias mortales — son absolutamente normales dadas las limitaciones de la IA. De ahí que esta necesite, para aprender, la ayuda humana: científicos de datos afinando parámetros y trabajadores de menor rango que se dedican a corregir clasificaciones, a sacar a los chihuahuas y a las magdalenas del mismo saco o a poner las etiquetas correctas a cada tipo de objeto o categoría.

¡Qué decepción! La IA no es solo matemáticas, ni funciona por arte de magia. Lo hace gracias a las hordas de trabajadores subcontratados a través de plataformas como Amazon Mechanical Turk, personas que a menudo trabajan en condiciones precarias, cobran una miseria y realizan tareas alienantes[*]. Algunas simplemente se pasan las horas resolviendo *captchas*: unas molestas pruebecitas que se presentan como paso final al realizar numerosas transacciones *online*. Por ejemplo, reconocer y escribir los números y letras que aparecen distorsionados en la pantalla, realizar una suma obvia o seleccionar casillas que contengan un objeto determinado (como un semáforo, una palmera…). Son pruebas automatizadas que los humanos pueden superar con facilidad, pero los algoritmos no. Y no solo las realizan personas a cambio de una remuneración, sino millones de usuarios —como usted y como yo— en sus operaciones diarias en internet.

ESPEJO SOCIAL

Lo anterior nos lleva a otro de los factores causantes del sesgo algorítmico. ¿A qué nos referimos con «sesgo algorítmico»? Es un tipo de error sistemático que puede suceder en sistemas informáticos (incluidos los basados en inteligencia artificial) al realizar suposiciones prejuiciosas. Si no se corrigen, su aplicación a casos reales dará

lugar a resultados incorrectos, injustos y negativamente discriminatorios, como ya hemos visto.

En la mayoría de los casos no hablamos de discriminación intencionada, sino de problemas de sesgo en las bases de datos de las que se alimentan los sistemas algorítmicos, que carecen de representatividad. Las personas hemos evolucionado mucho en cuestiones de discriminación, pero los datos usados son históricos, no disciernen entre nuestros valores pasados y actuales. Además, el hecho de que ahora estemos mejor no quiere decir que nos encontremos libres de sesgos: aún funcionamos como sociedades discriminatorias.

Otro gran escollo es la falta de diversidad entre los desarrolladores de tecnología, que en su gran mayoría son hombres blancos de clase media o media-alta, salvo la fuerza de trabajo subcontratada en otros países. También falta inclusión de perfiles de otras disciplinas. Como señala la experta Gemma Galdon: «Los ingenieros no pueden codificar un mundo que no entienden».[39]

Pero el mayor problema es social: mientras la discriminación siga estando presente en nuestra cultura, seguirá reflejándose, reproduciéndose y amplificándose en la tecnología. Como dice la socióloga y antropóloga Ruha Benjamin, la discriminación computacional no es un fallo en el sistema, sino parte de su arquitectura central.[40] Al verlo como error, se trata de arreglar con más y supuestamente mejores datos, en lugar de retroceder y pensar si es posible crear algoritmos justos en una sociedad injusta. Es un espejo al que no nos queremos mirar.

Tecnologías que a menudo se presentan como objetivas refuerzan el racismo y otras formas de inequidad. Si bien la segregación formal puede haber estado prohibida durante mucho tiempo, estos sistemas que recopilan datos a una escala sin precedentes facilitan nuevas formas de segregación más insidiosas y ocultas a la vista.[41] Sus propios creadores ignoran cómo la discriminación está codificada en unas tecnologías que prometen crear un mundo mejor.

Esta realidad es a menudo invisible también para aquellas personas de grupos privilegiados de la sociedad que no se ven negativamente afectadas por ello. Pueden ser eventualmente blanco de anuncios más caros debido a su estatus, pero no entrarán en los ciclos tóxicos de retroalimentación. Lo explica bien Eubanks:

> Los grupos marginados son objeto de niveles más altos de recopilación de datos cuando acceden a ayudas públicas, caminan por vecindarios altamente vigilados, entran en el sistema de atención médica o cruzan las fronteras nacionales. Esos datos actúan para reforzar su marginalidad cuando se utilizan para detectar sospechas y un escrutinio adicional. Aquellos grupos considerados indignos son seleccionados como blanco de políticas públicas punitivas y una vigilancia más intensa, y el ciclo comienza de nuevo. Es una especie de señal de alerta colectiva, un ciclo de retroalimentación de la injusticia.[42]

Eubanks sostiene que George Orwell se equivocó en una cosa en su novela *1984*: el Gran Hermano no le está mirando a usted, nos está mirando a nosotros. La mayoría de las personas son objeto de escrutinio digital como miembros de grupos sociales,

no como individuos. Las personas de color, los migrantes, los grupos religiosos impopulares, las minorías sexuales, los pobres y otras poblaciones oprimidas y explotadas soportan una carga de vigilancia y de seguimiento mucho mayor que los grupos favorecidos.

Aun así, nadie se escapa al ojo que todo lo ve en la era del «feudalismo digital». De cómo nos vigilan y nos controlan, de qué se oculta en las cloacas del autoritarismo *online* y de cómo funciona y cómo se ejerce el poder en la era del «capitalismo de la vigilancia»[43] hablaremos en el siguiente capítulo.

7

Tiranía digital

> *Un Estado totalitario realmente eficaz sería aquel en el cual los jefes políticos todopoderosos y su ejército de colaboradores pudieran gobernar una población de esclavos sobre los cuales no fuese necesario ejercer coerción alguna por cuanto amarían su servidumbre.*
>
> ALDOUS HUXLEY, *Un mundo feliz*, prólogo

> *Estamos siendo condicionados a obedecer. Más específicamente: estamos siendo condicionados a querer obedecer.*
>
> BRETT FRISCHMANN y EVAN SELINGER, *Re-engineering Humanity*

Panóptico. Una idea sin precedentes para controlar la mente. Un invento concebido para gobernar una prisión en el Reino Unido de finales del siglo XVIII, que ha acabado gobernando el mundo en el siglo XXI. Una inquietante propuesta inspirada en la Rusia zarista del príncipe Grigori Potemkin.

Samuel Bentham trabajaba para Potemkin. De él aprendió el «principio de inspección central» para mantener controlados a los trabajadores. Cuando se lo contó a su hermano —el filósofo y economista inglés Jeremy Bentham, padre del utilitarismo— este quedó fascinado. Con esa idea Jeremy concibió el panóptico: una penitenciaría en forma circular, con las celdas de los prisioneros dispuestas alrededor de la pared exterior y el punto central dominado por una torre de vigilancia. Desde la torre, el vigilante podía mirar las celdas en cualquier momento, pero los presos nunca podrían verle.

Jeremy Bentham pensó que los prisioneros, con la sensación de supervisión constante, modificarían su comportamiento y trabajarían arduamente para evitar cualquier castigo. Estaba convencido de que este modelo podría aplicarse efectivamente a diferentes instituciones. Así lo escribió:

> La moral reformada, la salud preservada, la industria vigorizada, la educación generalizada, las cargas públicas aligeradas; la economía asentada, por así decirlo, sobre una roca; el nudo gordiano de las Leyes de los Pobres no cortado, sino desatado, ¡todo gracias a una simple idea arquitectónica![1]

Una simple idea que ha traspasado, en efecto, las fronteras de la prisión, y también las de lo analógico a lo digital. Es la historia de cómo el diseño de un edificio se convirtió en el diseño de la sociedad subyugada. La misma historia que describió el

filósofo francés Michel Foucault, que ilustró con el panóptico la inclinación de las sociedades disciplinarias a someter a sus ciudadanos. Una realidad que George Orwell ya había descrito en su novela *1984*, en la que la vida transcurre en continua observación por parte del Gran Hermano.

Hoy, ese ojo que todo lo ve es internet, plagado de vigilantes no solo de la actividad *online*, sino de la *offline*, gobernado por unos pocos «grandes hermanos». Cada rincón cibernético registra nuestros movimientos, nuestros datos más íntimos, que son usados con fines económicos y políticos. El rudo capitalismo de la Revolución Industrial en la que vivieron los hermanos Bentham es en la actualidad una versión perfeccionada. Es el capitalismo de los gigantes tecnológicos que marcan las reglas del juego, que filtran lo que vemos y leemos, y que creen conocernos mejor que nosotros mismos.

En su imprescindible *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder*, la economista y profesora emérita de Harvard Shoshana Zuboff denomina a este sistema «capitalismo de vigilancia». Sigue siendo capitalismo, pero bajo una nueva lógica económica regida por el aparato digital. Un patrón que se aleja de la democracia de mercado y que da forma al entorno moral y político de la sociedad del siglo XXI y a los valores de nuestra civilización; que, sin ser violento, ejerce una violencia sutil: invade, viola y se apropia de nuestra intimidad.

Zuboff sitúa los comienzos de este modelo en el nacimiento de Google (2001). En concreto, en su sistema de ingresos publicitarios mediante el acceso exclusivo a registros de datos de navegación de los usuarios. La búsqueda de patrones predictivos de dichos individuos que coincidieran con los anuncios se hizo cada vez más agresiva, hasta encontrar nuevas fuentes de datos: aquellos que los usuarios habían optado por mantener en privado. De ellos se podía inferir una amplia información personal que estos nunca habían proporcionado.

La experiencia humana privada se convertía así en materia prima para el mercado, traducida en datos de comportamiento. No solo saben cómo navegamos en internet, qué buscamos o cómo nos comportamos en redes sociales. El panóptico que todo lo ve, tolo lo escucha y todo lo lee abarca cada sonido, cada texto e imagen, cada movimiento, cada conversación y cada expresión facial.

La ubicuidad de internet lo ha hecho posible. Dispositivos conectados que nos acompañan todo el tiempo junto con sensores, cámaras de vigilancia y sistemas de reconocimiento facial por doquier forman parte del aparato extractivo digital que nos vigila, controla y domina. Un sistema que busca, rastrea, extrae, almacena y procesa sin parar datos conductuales. Y que luego los transforma en predicciones sobre cómo se comportarán los usuarios: ellos, usted y yo. El panóptico de Bentham y el Gran Hermano de Orwell elevados a su máxima potencia.

Este cambio fue un punto de inflexión histórico. El sueño de una fuente de ingresos de coste cero. Un modelo envidiado que pronto se extendió a Facebook y se

convirtió en el sistema por defecto —una máquina de hacer dinero— en cualquier aplicación nacida en la meca de la tecnología, Silicon Valley. Un modelo ya globalizado y extendido a todos los sectores económicos, conocido como «colonialismo de datos».

Su alcance y capilaridad hacen que, aunque alguno de los máximos exponentes del capitalismo de la vigilancia desaparezca, otros llegarán para llenar su vacío. Se ha convertido en el capitalismo a secas. Y lo ha hecho embaucándonos, convirtiéndose en imprescindible para nuestras vidas conectadas a cambio de comodidad, de conocimiento y de cualesquiera otras recompensas.

La servidumbre llega hasta tal punto que los más pequeños descubren horrorizados, cuando crecen, que sus padres han compartido información e historias muy íntimas sobre ellos durante años. Algunos menores acaban incluso denunciando a sus progenitores.[2] No solo estamos regalando nuestras vidas al capitalismo de vigilancia, sino también las de nuestros hijos.

El panóptico del siglo XXI persigue el control de la población y este se materializa en formas de tiranía digital y vigilancia camufladas con excusas como la personalización de productos o servicios, la seguridad nacional, la comodidad, la salud pública, la mayor eficiencia de mercado y el aumento de la productividad, la protección para no herir sensibilidades, la lucha contra el discurso de odio o el orden social. ¿Cómo se materializa todo ello? Lo veremos, punto por punto, a continuación.

CONTROL DEL RASTRO *ONLINE*

La trampa de la personalización

Algunos de los datos *online* con los que comercian las empresas empezaron a recogerse supuestamente para mejorar los productos y servicios digitales: para personalizarlos y adaptarlos a cada usuario. Era y sigue siendo la excusa perfecta para extraer nuestros datos más íntimos. ¿Qué datos exactamente? Nuestro historial de búsqueda (que puede reconstruirse incluso aunque lo borremos). Lo que cada uno de nosotros ve, mira o escucha. Cualquier cosa que hayamos buscado por cualquier motivo (que, por sensible o íntimo que sea, se vincula con nuestra persona bajo categorías como «incesto», «abuso de drogas», «infertilidad», «salud mental» o si somos de izquierdas o de derechas).[3] Nuestro identificador numérico (ID) oculta nuestra identidad de forma seudonimizada, pero permite que se nos reconozca con ese número en las siguientes visitas.

Extraen también dicho ID asociado al perfil de cada uno de nosotros que tienen los compradores de anuncios. Nuestra geolocalización. Una descripción de nuestro dispositivo. Y, en algunos casos, hasta nuestra dirección IP, un identificador único que pertenece al dispositivo desde el que se conecta el usuario en concreto y que, por tanto, pueden vincular con nuestro nombre y apellidos.[4]

¿Adónde van a parar estos datos? A miles de terceros. Cuando una persona visita

una web cualquiera, los datos de su perfil *online* se envían a un servidor de anuncios. Después llegan a un sistema de oferta de espacios publicitarios e impresiones. Luego recalan en otro sistema de intercambio de anuncios que conecta los datos de las demandas de los anunciantes con los de los espacios publicitarios. Finalmente, una de esas demandas de anuncio segmentado será escogida y se mostrará al individuo que realiza la búsqueda. El sistema obtendrá de éste nuevos datos para completar la información que ya tiene sobre él (es decir, sobre todos nosotros, los usuarios), y así sucesivamente.

La filtración de datos no es exclusiva de Google. Apple, abanderada de la privacidad, también tiene fugas. Mientras dice que «lo que pasa en tu iPhone se queda en tu iPhone», la realidad muestra que otros tantos miles de terceros pueden acceder a los datos de los usuarios de un *smartphone*. Una investigación del columnista de tecnología Geoffrey A. Fowler (*The Washington Post*) junto con la empresa de privacidad Disconnect descubrió que había cinco mil cuatrocientas empresas rastreando su iPhone por semana, compartiendo con terceros un millón y medio de *gigabytes* de datos en solo un mes.[5] Entre ellos podrían estar su número de teléfono, su correo electrónico, su localización exacta o su huella dactilar. Entre las aplicaciones que compartían sus datos estaban Spotify, Nike, Microsoft OneDrive, Weather Channel o el propio *The Washington Post*.

Son aplicaciones que están funcionando en segundo plano, sin que el usuario sea consciente de ello.[6] Pueden incluso realizar capturas de pantalla cada cierto tiempo y enviarlas a un servidor externo. Como se ha demostrado, hay aplicaciones de aerolíneas, hoteles, agencias de viajes o bancos que graban en secreto la pantalla del iPhone e incluso exponen datos confidenciales de forma inadvertida.[7]

Darle a una aplicación acceso a la cámara significa darle el control para sacar fotos o grabar vídeos sin autorización expresa. Teóricamente, esto no pasa cuando solo aceptas que dicho acceso se produzca mientras usas activamente la *app*, pero eso es solo en teoría. Puede no ser así, bien de forma intencional, bien por error, como ocurrió con un fallo en la aplicación de videollamadas FaceTime que permitía escuchar a los contactos antes de que descolgaran el teléfono.

En el caso de Apple, el trazado de datos es posible gracias a su identificador IDFA para anunciantes. Es un código de seguimiento que permite a la empresa de la manzana y a todas las aplicaciones del teléfono rastrear a un usuario y combinar información sobre su comportamiento *online* y móvil.[8] Según la legislación de la Unión Europea, esto requeriría el consentimiento de los usuarios. Apple —hasta hace poco— no lo pedía, y por ello fue denunciada.[9]

Miles de terceros compran información disponible sobre nosotros. Cuanta más tengan, más completo será su perfil de cada usuario. Y usarán esa información como valor predictivo para manipularnos en su beneficio. ¿Para qué? No es para proporcionarnos mejores experiencias o cosas que nos gustan, pues eso es secundario y solo importante como medio para el fin primario: que compremos más o que

permanezcamos más tiempo en su plataforma. Por ejemplo, al ver una serie *online* en plataformas como HBO o Netflix, éstas nos sugieren otras series —de algún modo relacionadas con algo que hayamos visto anteriormente— que podrían gustarnos. Con ello nos inducen a ver más series y nos mantienen conectados, consumiendo.

Amazon hace lo propio. Además de rastrear las compras y la actividad de cada persona en su web o sus ubicaciones, registra sus hábitos de lectura hasta límites insospechados: cuánto avanzan y cómo progresan los usuarios con cada libro, qué partes de cada obra resaltan, qué extractos copian, con qué frecuencia buscan definiciones de palabras en el diccionario de Kindle y otras acciones en los dispositivos de lectura.[10] Son datos de los que se pueden hacer inferencias sobre la salud personal, la profesión, los rasgos personales o los pasatiempos de cada lector o lectora; una información que —dicen— solo usan para mejorar las experiencias de esas personas y sugerir otros libros que podrían gustarles.

Es la trampa de la personalización, el truco perfecto para conservar nuestra atención y seguir moviendo la rueda de consumo. Los algoritmos no se adelantan a nuestros deseos, sino que los modelan. Inhiben la creatividad, repitiendo y proponiendo el mismo tipo de patrón que ya se ha dado en el pasado, no algo nuevo (que también podría ser conveniente, interesante, bueno o de nuestro gusto).

Los ejemplos anteriores pueden parecer inofensivos pero, en el caso de plataformas de entretenimiento como Netflix, es el tipo de comportamiento que deriva en adicción. La mal llamada «personalización» no solo no va en nuestro beneficio, sino que directamente nos perjudica. Amazon dice no compartir los datos de lectura de sus usuarios con terceros, pero eso no significa que no pueda hacerlo.

Más flagrante es el caso del sistema operativo de Google, Android. Una investigación de más de ochenta y dos mil *apps* preinstaladas en más de mil setecientos teléfonos Android de más de doscientos fabricantes reveló que dicho sistema operativo ha facilitado comportamientos potencialmente dañinos y el acceso oculto a datos y servicios confidenciales sin el consentimiento o conocimiento de los usuarios.[11]

Otro análisis de mil aplicaciones para teléfonos Android encontró que el 61 por ciento de ellas comparte información con Facebook de forma instantánea en el momento en el que un usuario abre la aplicación, sin preguntarle y sin importar que este tenga o no una cuenta en dicha red social.[12] ¿Más ejemplos? Escriba en uno de sus grupos de WhatsApp «Vamos de vacaciones a Nueva Zelanda» y compruebe cuánto tarda Facebook en mostrarle anuncios de rutas por las antípodas.

Facebook controla a los usuarios incluso cuando estos no tienen la aplicación abierta. Sabe qué páginas ha visitado cada persona y durante cuánto tiempo. ¿Cómo lo hace? A través de los botones de «Me gusta» que se cargan en todas las páginas web que visitamos y que envían a Facebook el registro de esa visita, independientemente de que hagamos clic en ellos o no.

Para alimentar sus algoritmos, su IA, Facebook recopila datos allá donde pueda con tal de atraer a más usuarios y de mantenerlos ahí por más tiempo; unos datos que, además, sí que intercambia con terceros. Un arrepentido inversor y exasesor de la empresa reconoció que «en poco tiempo [desde su creación], Facebook estaba espiando a todos, incluidas las personas que no usaban Facebook».[13]

Estás ahí aunque no quieras. «No tener una cuenta en la red social no lo resuelve, porque la herramienta también obtiene datos de personas no registradas a través de personas que sí lo están», me contaba en una entrevista[14] Max Schrems, el abogado austriaco que inició un juicio contra Facebook por su actividad de rastreo en 2013, cuando aún no había terminado siquiera la carrera. Un juicio que ganó ante el Tribunal de Justicia de la Unión Europea y que invalidó el acuerdo Safe Harbor de transferencia de datos personales entre la Unión Europea y Estados Unidos.

CONTROL DE MOVIMIENTOS Y VIGILANCIA PARA LA SEGURIDAD NACIONAL, LA SALUD PÚBLICA Y LA COMODIDAD DOMÉSTICA

La envidia de 007

Schrems presentó varias denuncias contra Facebook a raíz de las revelaciones de Edward Snowden sobre la cooperación de Facebook con agencias de seguridad de Estados Unidos como la CIA o la NSA. Snowden, por si no lo recuerdan, es el joven estadounidense que expuso el sistema de vigilancia masiva del Gobierno de Estados Unidos.[15] El desengaño al descubrir que «el Gobierno era el enemigo»[16] le llevó a pasar de espía a denunciante. Él mismo —como empleado que fue de la CIA y la NSA— formaba parte de ese sistema que registra en secreto cada llamada telefónica, cada mensaje de texto y cada correo electrónico de los ciudadanos. Una arquitectura de espionaje sin precedentes con la capacidad de indagar en la vida privada de cada persona en la Tierra.[17]

Es un sistema que no solo se ha hecho obvio, sino que no oculta su alcance, con gobiernos democráticos que han legalizado el registro tanto de llamadas como de metadatos de internet (información que describe otra información para ayudar a comprenderla o usarla). Un ejemplo de metadato son las etiquetas que ponen las cámaras digitales a las imágenes: título, descripción, categorías… En un *e-mail*, los metadatos son el asunto, quién lo envía y a quién o quiénes, fecha y hora de envío, nombres del servidor y dirección IP (Internet Protocol), etc.

Una dirección IP vinculada con información básica sobre un suscriptor de servicios de telecomunicaciones es suficiente para revelar los intereses de una persona, sus inclinaciones, con quién se asocia o adónde viaja. Los metadatos son, de hecho, tan peligrosos contra la privacidad como lo puede ser el propio contenido de los mensajes. Este tipo de dato se recopila y se acumula a lo largo del tiempo para ser añadido y obtener información relevante. Dada la capacidad actual de almacenar datos masivos y de procesarlos, es posible cruzar muchos de esos metadatos.

De esta forma, además de obtener información privada, pueden detectarse patrones —algo en lo que los sistemas de inteligencia artificial son expertos—, amén de trazar un mapa de relaciones o realizar inferencias íntimas. Por ejemplo, es posible crear un gráfico de la red humana en torno a un individuo específico, identificando a todas las personas a uno o dos grados de separación de él. Es lo que se llama el «grafo social» de un individuo.

La combinación de información sobre nuestras relaciones en redes sociales, los datos sobre nuestra ubicación que salen de las torres de telefonía móvil, los metadatos de nuestros correos electrónicos o el rastro de los productos que compramos *online* pueden pintar una imagen profundamente detallada de nuestras vidas.[18] Casi todas las actividades *online* dejan algún tipo de rastro personal que va a parar a un gran universo de metadatos que no resulta difícil correlacionar.

Esta información representa, de forma agregada, un marcador de posición para las intenciones de la humanidad: una base de datos masiva de deseos, necesidades y preferencias que se pueden descubrir, citar, archivar, rastrear y explotar para todo tipo de fines.[19] Incluso para matar. «Matamos a gente sobre la base de metadatos», aseguró el exdirector de la NSA y la CIA Michael Hayden durante un debate en 2014.[20]

Como hemos visto, incluso los términos que escribimos en buscadores pueden usarse para identificarnos y revelar información confidencial sobre nosotros. Hay muchas formas posibles en las que terceros pueden conocer información íntima sobre nosotros. Por ejemplo, se puede averiguar la identidad de nuestro cónyuge a partir de la estructura de contactos de una persona en Facebook[21] (sin necesidad de conocer el contenido de su perfil). Es posible también predecir los datos demográficos de los usuarios (género, tipo de trabajo, estado civil, edad y el número de miembros de la familia) mediante datos móviles;[22] una información que, por otro lado, recopilan por defecto aplicaciones de todo tipo: de transporte, de reparto de comida a domicilio, supermercados, servicios de entretenimiento y música en directo, marcas de ropa, aerolíneas y un largo etcétera en el que se encuentran, a la cabeza, las redes sociales.

A partir de los metadatos es posible también inferir información más sensible relativa a nuestra salud. Por ejemplo, se puede saber que una persona tiene esclerosis múltiple a partir de metadatos que desvelan que esta mantiene comunicaciones con una farmacia especializada en cuidados crónicos, un servicio a pacientes con afecciones graves, varios servicios de neurología locales y una línea directa farmacéutica para un medicamento recetado que se usa únicamente para controlar los síntomas y la progresión de esa enfermedad.[23]

El perfilado *online* de los usuarios va más allá a medida que aparecen nuevas tecnologías conectadas. Los dispositivos *wearables* o «llevables» (en forma de brazaletes o de relojes inteligentes, entre otros) miden parámetros corporales y de actividad. Almacenan información íntima sobre nuestra salud, además de conocer nuestra localización en todo momento. Estos datos se comparten directamente con el

smartphone y otros dispositivos mediante *bluetooth*. La información se almacena en una cuenta personal en la nube *online*. Según quién los administre, aquella se puede vender, compartir o intercambiar estratégicamente con terceros y utilizarse —en el mejor de los casos— para enviar anuncios al usuario. Por no mencionar la posibilidad de pirateo en sistemas que a menudo no están bien protegidos.

Para más inri, en 2019 Google compró Fitbit, una de las pulseras de actividad más populares. Permitir que las capacidades de recopilación de datos de Fitbit se pongan en manos de Google crea grandes riesgos de explotación del consumidor y de monopolio.[24] La combinación de los datos de salud de Fitbit con otros de Google crea oportunidades únicas para la discriminación en la atención médica, los seguros médicos y otras áreas sensibles. Aunque Google mantenga su promesa de que la información de salud y de actividad de Fitbit no se usará para personalizar anuncios, otros datos como la localización pueden tener importantes implicaciones para la privacidad.

Quebraderos de cabeza similares traen otros dispositivos conectados para el hogar, desde aspiradoras hasta cafeteras. Un paso más allá van los altavoces inteligentes, que asisten en tareas como poner música o vídeos o buscar restaurantes o vuelos; que responden a consultas relacionadas con la actualidad, el tiempo o con cualquier cosa que se pueda buscar en internet.

Cómo no, Google comercializa uno de estos dispositivos, Google Home. También lo hace Amazon con su dispositivo Echo y su asistente Alexa. Estos juguetitos para el hogar expanden sensiblemente la vigilancia de la vida privada de los consumidores[25] de distintas formas. Pueden deducir sentimientos y comportamientos a partir de las voces que capte en el entorno, además de escuchar la voz humana —conversaciones telefónicas incluidas— para extraer contenido que pueda orientar la publicidad (por ejemplo, «Me encanta nadar»).

Pueden identificar interlocutores en una conversación y construir perfiles de interés para cada uno.[26] Con la promesa de adaptar sus servicios a la persona que habla, pueden usar perfiles de voz para asociar comportamientos (por ejemplo, horarios para dormir, cocinar, divertirse o ducharse) a individuos específicos en el hogar (de nuevo para encauzar los anuncios).

Pueden compartir datos con terceros, recomendar productos sobre la base del mobiliario observado por una cámara que también clasifica las características de los usuarios (género, edad, gusto por la moda, estilo, estado de ánimo, idiomas, actividades preferidas, etc.), o identificar la presencia de niños y los momentos de travesura, asimismo con aplicaciones publicitarias.[27]

Pueden espiar las conversaciones y, al mismo tiempo, cumplir técnicamente su promesa de almacenar y analizar solo las grabaciones de audio que el usuario pretende compartir.[28] Aun así, se ha demostrado que no lo hacen. Al menos, no siempre. Cuando en 2018 varios usuarios de Echo informaron de que Alexa se reía a veces sin venir a cuento, se encendieron las alarmas. La noticia dio la vuelta al

mundo, como lo hizo el relato de un matrimonio al que Alexa había grabado la conversación privada y se la había enviado a un contacto. Todo ello sin su permiso ni su conocimiento.[29]

La explicación de Amazon al respecto no hizo sino poner de manifiesto el mal funcionamiento del aparato y su imprecisión. A pesar de que la compañía trató de que esto se viera como un error puntual, la periodista Rachel Metz comprobó que la grabación de conversaciones sin permiso era algo sistemático.[30] En abril de 2019 varios empleados de la compañía desvelaron que un equipo de miles de trabajadores de Amazon escucha de forma aleatoria lo que los usuarios le dicen a Alexa.[31] No solo revisan los clips de audio, sino que transcriben y revisan fragmentos de conversaciones. Eso sí, lo hacen, supuestamente, para mejorar el funcionamiento del asistente. Todo sea por nuestro bien.

El revuelo y la indignación causados al revelarse todo esto hicieron que Amazon incorporase al dispositivo una función de borrado de las conversaciones, con opciones para eliminar todo lo que se ha dicho en un día o algo que se acaba de decir.

Estos sistemas de registro de voz, incluidos los asistentes virtuales integrados tanto en aparatos para el hogar como en *smartphones* y en vehículos, han demostrado ser verdaderos agentes de espionaje. Algo parecido sucede con Clubhouse, la aplicación reina del FoMO, que graba y guarda las conversaciones de los usuarios. Usted y yo no podemos acceder a ellas, pero Clubhouse sí. También recopila información sobre cada perfil. Cosas como con qué frecuencia y durante cuánto tiempo está activo cada usuario, en qué momentos del día se conecta y con qué personas y grupos se comunica. ¿Con qué fines? La transparencia brilla por su ausencia.

¿Se imaginan todas estas herramientas en malas manos? No es difícil hacerlo, dado que estos sistemas tienen vulnerabilidades de privacidad que son y serán aprovechadas por piratas informáticos con objetivos maliciosos. O incluso por usuarios comunes y corrientes, como el que sacó contenido de Clubhouse para retransmitirlo en su web sin ningún tipo de problema.[32] La Universidad de Stanford ya advirtió de fallos de ciberseguridad de la *app*.[33] También de que el tráfico de datos y la producción de audio de WhatsApp dependen de una empresa china llamada Agora.

Mención aparte merecen las tecnologías de biometría y reconocimiento facial. Las tecnologías biométricas se usan para verificar la identidad de los seres humanos sobre la base de una o más características físicas (rostro, huellas dactilares, iris) o de comportamiento (por ejemplo, su firma). Estas aplicaciones de autentificación que durante años han permanecido en el terreno de la seguridad nacional y la aplicación de la ley están hoy en todas partes. En especial, el reconocimiento, la detección y el análisis facial, que han llevado la vigilancia a una escala sin precedentes.

Esta tecnología afecta ya a la mitad de la población mundial de forma regular.[34] Está en uso en al menos noventa y ocho países y prohibida en tres.[35] Y ocupa nada

menos que el tercer puesto en la clasificación de inversión privada global en inteligencia artificial; en 2019 se llevó un 6 por ciento del importe total de lo invertido en ese campo, prácticamente lo mismo que lo que se dedicó a la aplicación de IA en medicamentos, cáncer y terapia.[36]

¿Para qué se usan los sistemas de detección de rostros? Comúnmente se hace con fines de verificación o identificación, desde usos policiales (identificar delincuentes o asistir en la búsqueda de personas desaparecidas) hasta otros más aparentemente nimios, como desbloquear el *smartphone*. Están plenamente integrados de forma rutinaria en nuestras vidas. Hasta Mercadona los usa —no sin polémica— en sus supermercados.[37]

Por la sensibilidad del contenido que manejan, el uso de sistemas de reconocimiento facial es muy criticado y cuestionado. Por ello se hace a menudo de forma oculta. Por ejemplo, se sabe que en Estados Unidos la policía inserta fotos de redes sociales de acusados en programas de reconocimiento facial para identificarlos. De hecho, varias investigaciones periodísticas han revelado que la empresa Clearview AI recopiló miles de millones de imágenes de redes sociales y sitios web para crear un motor de búsqueda de rostros, y luego autorizó su uso a más de seiscientas agencias policiales de Estados Unidos.[38] Eso además de a particulares, a bancos, a escuelas o a minoristas.[39]

Ahí estaba esa pequeña *startup* haciendo algo que las grandes tecnológicas capaces de lanzar una herramienta de este tipo no se habían atrevido a llevar a cabo. No porque no fuera tentador sino, por hipócrita que parezca, por su evidente agresión contra la privacidad y las posibilidades de uso indebido.

¿Cómo funcionan estas tecnologías? Para la verificación, comparan los rasgos faciales de una persona con las imágenes disponibles para confirmar que una foto coincide con otra de una credencial o con un retrato diferente de la misma persona en un archivo fotográfico. Para la identificación, determinan si la persona de la foto presenta coincidencias con una base de datos.

Como hemos visto en el capítulo anterior, lejos de ser perfectas, las herramientas de análisis facial fallan más que una escopeta de feria. Los errores de estos sistemas tienen serias consecuencias: arrestos indebidos,[40] sistemas de identificación de sospechosos que se equivocan el 80 por ciento del tiempo,[41] herramientas policiales de detección que fracasan el 96 por ciento de las veces,[42] tecnologías para reconocer pasaportes que no identifican a personas de piel oscura[43] o discriminación sistemática de personas de color en redes sociales.[44]

Los errores de distinción por raza son, de hecho, frecuentes en los sistemas biométricos. La investigadora Joy Buolamwini los sufrió en sus propias carnes cuando cursaba su posgrado en el laboratorio Media Lab del Instituto Tecnológico de Massachusetts (el MIT, en Estados Unidos). Allí trabajaba con aplicaciones de reconocimiento facial en diferentes proyectos, pero dichos programas no reconocían correctamente su rostro, y eso le impedía usarlos. Joy pudo solventar el problema de

forma analógica. La solución: se puso una máscara blanca. Aquello le llevó a reconducir su trabajo y a investigar sobre el asunto. Así descubrió que el problema era aún mayor si se combinaban las variables de raza y género: la tasa de error aumentaba para las mujeres negras.[45]

Razas aparte, hay otras muchas razones por las que los sistemas biométricos pueden fallar. Tanto su eficiencia como su precisión pueden verse significativamente afectadas por múltiples variables demográficas, como el género, la edad, las gafas o la altura,[46] además de la iluminación, la variación de la pose o las expresiones faciales.

Por ello, es altamente probable que los sistemas de reconocimiento facial no funcionen de manera adecuada u óptima. Tras dos décadas de investigación continua, así como de mucho dinero y esfuerzo puestos en ello, no son todavía lo suficientemente precisos ni eficientes.[47] La letra pequeña sobre sus límites a veces se pasa por alto y tienden a tener pocos requisitos de precisión.

Estas tecnologías que a menudo resultan poco efectivas se pagan con dinero de los contribuyentes. Los estados son grandes compradores de herramientas de vigilancia. La joya de la corona es el reconocimiento facial, aunque también abundan las plataformas de seguridad para ciudades inteligentes y los sistemas policiales.[48]

China es uno de los principales impulsores mundiales de la vigilancia inteligente o basada en inteligencia artificial. Empresas chinas como Huawei, Hikvision, Dahua o ZTE suministran este tipo de herramientas a setenta y tres países.[49] Entre ellos no solo se encuentran gobiernos autoritarios. Las democracias liberales son, de hecho, los principales usuarios de estas tecnologías. El 51 por ciento de las democracias avanzadas implementan estos sistemas de vigilancia inteligente frente a menos de un 41 por ciento de estados autocráticos.[50] Estos últimos son más propensos, eso sí, a abusar de la vigilancia, a menudo con fines represivos o para conseguir ciertos objetivos políticos. China, Rusia o Arabia Saudí[51] y otros gobiernos con pésimos antecedentes en materia de derechos humanos son un ejemplo de implantación de sistemas masivos de vigilancia represiva.

Estados Unidos es otro de los grandes productores y exportadores de tecnologías de vigilancia y espionaje. Cisco, IBM, Herta y Palantir son algunas de las empresas más destacadas. España es cliente de IBM y Herta, de la israelí NSO y de otras como la china Huawei.[52] Es posible que lo sea también de Palantir, que ofreció sus servicios al Gobierno español[53] para ayudar a manejar la pandemia del coronavirus.

Palantir es una de las muchas empresas que han aprovechado la crisis para sacar tajada y ampliar su presencia en Europa. El Reino Unido contrató a esta compañía para proporcionar a su sistema de salud (NHS) paneles de control interactivos sobre la base de los datos de disponibilidad de recursos e infraestructura que ya posee (cosas como qué ventiladores se están utilizando y dónde, niveles de enfermedad del personal, número de camas disponibles, etc.).

Sin embargo, documentos internos del proyecto mostraron que la empresa podía acceder a información sensible, a grandes volúmenes de datos clínicos protegidos.[54] Es algo preocupante teniendo en cuenta que la experiencia de Palantir no reside en la gestión de datos de salud pública, sino en el análisis de datos para el espionaje (creando productos para las agencias de inteligencia y defensa de Estados Unidos). Su nombre, de hecho, alude al Palantir de *El señor de los anillos*, una especie de bola de cristal todopoderosa para vigilar a enemigos.

Palantir no es ni mucho menos la única empresa que ha aprovechado la COVID-19 para ampliar influencias y hacer dinero. Cual martillo que solo ve clavos, muchas compañías han creído tener la solución a algunos de los retos de la pandemia, o así han intentado que parezca. En gran parte de los casos han reutilizado tecnología existente para abordar preocupaciones específicas del coronavirus. En otros, han aprovechado la ocasión para conseguir financiación para desarrollar nuevos productos relacionados con su área de trabajo.

Lo anterior, que no tiene por qué ser negativo *per se*, ha servido como excusa para amplificar la vigilancia. Se han instalado cámaras termográficas en comercios, empresas y escuelas; unas cámaras que no son lo bastante precisas si no se calibran bien y que pueden discriminar injustamente (a menudo sin motivo, dado que una persona puede tener la temperatura alta por muchas causas ajenas al coronavirus). Se ha justificado el uso de tecnologías que invaden la privacidad y de sistemas de control laboral, tanto desde el sector privado como desde el público. Se ha invertido dinero público en el desarrollo de sistemas de rastreo de contactos o de reconocimiento facial para detectar quién lleva o no mascarilla, y la policía ha comenzado a usar drones patrulla para hacer cumplir la cuarentena.

Son ejemplos del abordamiento del solucionismo tecnológico contra la pandemia en España, pero la COVID-19 no es la única razón para incrementar la vigilancia tecnológica en nuestro país y el uso de sistemas de reconocimiento facial a menudo injustificados o innecesarios. Hasta el aeropuerto Adolfo Suárez Madrid-Barajas inició en 2021 una prueba piloto de reconocimiento facial para —según dice— mejorar la seguridad y agilizar los viajes aéreos. También se abrió la puerta en 2020 a la posibilidad de instalar sistemas de reconocimiento facial como herramienta de control en eventos multitudinarios para facilitar que los agentes puedan detener a personas con asuntos pendientes con la justicia.[55] Casi un año antes se anunciaba un proyecto piloto para el uso de un sistema de reconocimiento facial que permita pagar en los autobuses de la ciudad de Madrid.

En países como China, los ejemplos de uso de herramientas digitales para la vigilancia son más extremos. El Gobierno chino aprovechó la emergencia para intercambiar a puerta cerrada datos personales con empresas privadas.[56] También desarrolló un sistema digital de control social para determinar quién podía subir a un tren o entrar en un edificio, dependiendo del color que una *app* asignase a cada persona.

La COVID-19 ha traído todo un nuevo nivel de vigilancia masiva. Tanto que hay quienes, como Albert Fox Cahn, director del Surveillance Technology Oversight Project, califican este momento como «el más peligroso para los derechos civiles desde el 11-S».[57] Ante decisiones como mantener abiertas las escuelas o no, y privar a los niños de la educación o ponerles en riesgo, es muy fácil dejarse engañar por el encanto del pensamiento mágico y las nuevas empresas que dicen que, solo con instalar su dispositivo o usar su aplicación, se podrá evitar el dilema.

CONTROL LABORAL

Precari@s bajo demanda

Del control social al control laboral. A raíz de la pandemia se instalaron en los puestos de trabajo no solo las ya mencionadas cámaras térmicas con reconocimiento facial, sino también dispositivos portátiles que rastrean los movimientos de los empleados y monitorean las violaciones del distanciamiento social. Otro recurso son los sistemas que controlan a los trabajadores en remoto, en un momento de florecimiento del teletrabajo. Estas herramientas de vigilancia permiten registrar las pulsaciones de teclas o capturar la pantalla de los empleados,[58] o incluso los obligan a mantener la cámara siempre activa.

Otras tecnologías controlan a los trabajadores de formas menos obvias, pero igualmente dañinas. Este control es uno más de los elementos en los que se basa la tiranía digital enraizada en la economía de los minitrabajos o *gig economy*.

La conectividad permanente, junto con la generalización de los *smartphones* y el mercado de las aplicaciones móviles, impulsó un nuevo modelo de consumo: la economía bajo demanda. El esquema es sencillo: ahora lo necesito, ahora lo pido, ahora lo tengo. Y el trabajo lo hará quien esté disponible en ese momento.

Esta economía engloba servicios de entretenimiento en directo, como Spotify o Netflix, y plataformas de intercambio y de acceso u ofrecimiento de todo tipo de cosas: bienes y productos (como Airbnb o Amazon), servicios (como Cabify o Glovo), fuerza de trabajo (como TaskRabbit o Amazon Web Services) o contactos, amistades o contenidos (como Facebook, Twitter o Tinder, por citar solo algunas).

Algunas de estas plataformas tuvieron sus orígenes en la llamada «economía colaborativa» entre pares, que no implicaba por fuerza una contraprestación y que venía asociada a una serie de valores de anticonsumismo y aprovechamiento eficiente y sostenible de bienes y recursos infrautilizados. Pronto ese modelo, del que nacieron Airbnb, Uber o Glovo, derivó hacia usos más comerciales y altamente lucrativos.

Como Google, estas empresas supieron ver el vacío regulatorio en el salvaje Oeste del trabajo bajo demanda *online* mediado por plataformas y *apps*. Con base en él diseñaron un nuevo modelo de negocio con un coste cercano a cero cuyo beneficio no se apoyaba en el excedente de datos, como Google, sino en el ahorro: de costes de

producción, distribución e intermediarios, así como de gastos laborales asociados a las formas de empleo tradicionales.

Lo plasma muy bien la famosa frase del directivo de Havas Media Tom Goodwin: «Uber es la compañía de taxis más grande del mundo y no tiene vehículos. Facebook es el propietario de medios más popular del mundo y no crea contenido. Alibaba es el minorista más valioso y no tiene inventario. Y Airbnb, el mayor proveedor de alojamiento del mundo, no tiene propiedades inmobiliarias», aseguró allá por 2015.

A pesar de no tener nada, estas empresas lo tenían todo. El *quid* de la cuestión es que para ello se estaban aprovechando de los bienes y servicios de otros, y —según el caso— de una fuerza laboral supuestamente autónoma con la que carecían de vinculación contractual y por la que no debían rendir cuentas. Dado que a menudo estas plataformas se basan en una filosofía de bajo coste de márgenes muy ajustados, su modelo no permite una elevada remuneración por tarea o por tiempo de trabajo. Esto, junto con la ausencia de beneficios laborales como vacaciones o seguros de salud, ha derivado en un modelo de trabajo a menudo precario en el contexto de la economía de plataformas.

Son trabajadores a cuya precarización contribuyen también las formas de control a las que se someten, mediadas digitalmente. Su seguimiento y vigilancia es constante a través de la propia plataforma o *app*. Esta les asigna el trabajo, determina cuánto tiempo tardarán en realizarlo y les castiga cuando se desconectan o cuando obtienen valoraciones bajas. «En realidad no puedes decidir: si no te conectas, te baja la puntuación, y si no tienes más de un cuatro y pico, no te entran pedidos. Es muy tiránico, no eres realmente libre», comentaba en una entrevista para *El País* Isaac Cuende,[59] uno de los primeros trabajadores de la aplicación de reparto a domicilio Glovo (y el primero también en ganar un juicio contra la empresa ante el Tribunal Supremo al reconocer este último la condición de falsos autónomos de los repartidores).

Los jefes de tantas trabajadoras y trabajadores de plataformas como Cuende no son humanos: son algoritmos que determinan qué deben hacer, cuándo y cómo, e incluso pueden despedirles. Los algoritmos no tienen intenciones ni toman decisiones, pero ejecutan los comandos que sus diseñadores han programado. Y esas órdenes son a menudo perversas: el resultado de una fórmula matemática de optimización diseñada para maximizar la eficiencia y las ganancias de la empresa.

Lo que es propicio para la transacción puede no serlo para el operario, pero el código que hace funcionar estas plataformas y aplicaciones no tiene en cuenta el bienestar de los trabajadores. Entre estos y la *app* hay una asimetría de poder y también de información. A menudo los algoritmos trabajan como cajas negras y no se sabe con exactitud cómo funcionan. Esto hace que sea dificilísimo para los trabajadores impugnar decisiones o cambiar su comportamiento para poder mejorar. También invisibiliza los posibles sesgos. ¿Hasta qué punto es permisible que una

persona preparada no tenga acceso a ciertas tareas porque la plataforma no se las muestra?[60]

La cuestión no es hipotética, sino un problema frecuente. La discriminación algorítmica está presente en las aplicaciones bajo demanda cuyos algoritmos determinan también la fiabilidad de los trabajadores. Lo hacen mediante un ranking de reputación que tiene en cuenta, entre otras cosas, las cancelaciones de trabajo con menos de veinticuatro horas de antelación. Eso sin importar la causa, aunque esta sea una emergencia o una enfermedad grave. A quienes tienen índices de fiabilidad más bajos, se les asignan menos turnos de trabajo, lo que repercute directamente en su capacidad de obtener ingresos. Por ese motivo, un tribunal italiano determinó que la conducta de Deliveroo era ilegalmente discriminatoria. Ordenó a la empresa eliminar dichas prácticas y cualquier otra que obstaculizara el ejercicio de los derechos de los repartidores, así como indemnizar económicamente a las organizaciones sindicales demandantes.[61]

La gestión basada en aplicaciones amplifica la inseguridad y la inestabilidad de un trabajo que ya es de por sí precario. El vacío de información, la falta de mecanismos de retroalimentación y el control del desempeño basado en datos son los tres elementos centrales de la «precariedad digital».[62] A esto se le añaden tácticas para hacer que las trabajadoras y trabajadores dependan de la plataforma para ganarse la vida. Se les atrae con promesas de un salario digno y condiciones laborales flexibles para recortar después la remuneración de forma drástica, una vez que dichas personas hayan estructurado sus vidas en torno al trabajo para la plataforma.[63]

Otro efecto de este tipo de trabajo es el «techo algorítmico».[64] Así como el «techo de cristal» impide ascender a las mujeres en la jerarquía de las organizaciones, el techo algorítmico impide el avance profesional de las personas que se ganan la vida trabajando para las plataformas bajo demanda y que rara vez interactúan con otras personas por encima de ellas en la jerarquía de la compañía.

En circunstancias muy similares se encuentra otra tipología incipiente de trabajo en internet: la computación humana. Son labores que empiezan y terminan *online* y que realizan cualquier tipo de tarea que pueda ser administrada, procesada, efectuada y pagada en línea.[65] La mayoría de ellas tienen que ver con la inteligencia artificial (IA), sea para facilitar, supervisar o completar su desarrollo o para realizar tareas que esta no es capaz de hacer. Allá donde no llega la máquina entran los humanos. Por ejemplo —como hemos contado en el capítulo anterior—, para resolver *captchas*.

Se calcula que solo las tareas de etiquetado relacionadas con la IA supondrán un mercado global de más de cuatro mil millones de dólares a finales de 2024.[66] La digitalización y la robotización pueden destruir empleo o reemplazar a las personas en ciertas tareas, pero siguen creando trabajo. Es lo que la antropóloga Mary L. Gray denomina «la paradoja de la última milla de la automatización»: que el deseo de eliminar el trabajo humano siempre genera nuevas tareas para los humanos.

Estos trabajos —etiquetado, clasificación, identificación de discursos de odio, etc. — potencian los sistemas, sitios web y aplicaciones de IA que todos usamos y damos por sentado. TripAdvisor, Match.com, Google, Twitter, Facebook o la propia Microsoft son algunas de las empresas que echan mano de las trabajadoras y trabajadores *online*, que contratan a través de plataformas como Amazon Mechanical Turk; un tipo de trabajo «fantasma» que hace invisible la labor de cientos de millones de personas.[67]

Entre esas personas están también las que moderan el contenido de las redes sociales. Son las que deciden si una foto del cuadro *La maja desnuda* de Goya pasa el filtro de la censura antiporno de Facebook o si un vídeo de la violencia ejercida contra los inmigrantes en las fronteras es calificado como «contenido adulto» en YouTube o directamente eliminado por violento.

«En mi primer día de trabajo, fui testigo de cómo mataban a golpes a alguien con una tabla de madera con clavos y lo apuñalaban repetidamente», relató a *Vice* Sean Burke,[68] uno de los miles de moderadores de contenidos de Facebook. Un trabajo agotador a cambio de un salario mínimo que le llevó a consumir antidepresivos; a él y a otro puñado de trabajadores, que, en 2018, decidieron demandar a la red social por no protegerles de un posible trauma mental.

Los moderadores denunciaban ser bombardeados con miles de vídeos, imágenes y transmisiones en vivo de abuso sexual infantil, violación, tortura, bestialidad, decapitaciones, suicidio y asesinato. En 2020, Facebook acordó pagar 52 millones de dólares a un total de 11.250 personas que ejercían el trabajo en ese momento o lo habían ejercido con anterioridad.

La situación de estos trabajadores evidencia cómo se ha usado y se usa la tecnología de formas que contribuyen a la precarización y a la polarización del empleo. Ha ayudado de forma desproporcionada a profesionales con altas cualificaciones y ha reducido las oportunidades para muchos otros. Crece la desigualdad, la brecha entre quienes están más y mejor preparados para las demandas de trabajo y quienes han sido desplazados y se encuentran en la obligación de tener que aceptar ocupaciones precarias para sobrevivir, cuyas capacidades de negociación, además, disminuyen. Estas tendencias, lejos de extinguirse, corren el riesgo de exacerbarse a medida que se implantan y avanzan las nuevas tecnologías.

CONTROL DE INFORMACIÓN, PENSAMIENTO Y EXPRESIÓN

Censura y autocensura

La tiranía digital es vigilancia, pero también censura. Mientras los moderadores de contenido de plataformas *online* y redes sociales se juegan su salud mental para filtrar aquello que incumple las políticas de las empresas para las que trabajan, estas son denunciadas por eliminar vídeos, imágenes o textos de forma indebida.

Las redes sociales acumulan innumerables casos de cuestionable eliminación de contenidos. YouTube atesora gran parte de ellos. Se trata de un largo historial que lleva forjando desde que en 2007 suspendiera la cuenta de un prominente activista egipcio contra la tortura que compartía imágenes sobre brutalidad policial.

Las polémicas más recientes tienen que ver con la pandemia de coronavirus. Entre otros muchos casos, YouTube censuró un vídeo del dúo humorístico español Pantomima Full que parodiaba a los negacionistas de la COVID-19. Supuestamente se debió a un fallo de los algoritmos de la plataforma dedicados a buscar clips que contradicen las indicaciones de las autoridades sanitarias. Al parecer, estos no advirtieron que se trataba de una pieza de humor. Sin embargo, como denuncia la organización de verificación Maldita,[69] otros vídeos no humorísticos que intentan desincentivar el uso de la mascarilla o que difunden teorías de la conspiración no se retiran, e incluso se distribuyen en otras redes como Facebook.

Twitter o Instagram no se salvan. La primera ha sido objeto de quejas frecuentes por bloquear cuentas de forma injustificada y por suprimir noticias de forma errónea. Instagram, por su parte, es criticada a menudo por su arbitrariedad a la hora de eliminar desnudos. Por ejemplo, por quitar imágenes de la humorista Celeste Barber, conocida por caricaturizar posados imposibles de modelos de publicidad mediante fotos donde las imita, y mantener, sin embargo, los originales en los que se basa.[70] Lo de los desnudos no es anecdótico, sino sistemático, y es causa de censura indiscriminada de obras de arte. Contra esta realidad nació la campaña internacional «Don’t delete art»[71] («No borres el arte»): una galería *online* de arte censurado por redes sociales que, además, ofrece a todos los artistas compartir sus historias en una «censorpedia». Sus instigadores denuncian cuán a menudo el trabajo y las cuentas de artistas se eliminan por error y sin posibilidad de apelación, lo que puede conducir a la autocensura.

Lo de la aplicación china TikTok tampoco es para menos. Según documentos internos de la policía china obtenidos por *The Intercept*, los moderadores de la plataforma de vídeos cortos tenían instrucciones de suprimir las publicaciones de personas feas y pobres para atraer nuevos usuarios.[72] También tenían órdenes de bloquear emisiones en directo de contenido político crítico con China.[73]

A un nivel más macro, son los gobiernos los que lideran la censura *online*. En el capítulo 1 hemos visto ejemplos de cierres temporales o permanentes de internet o de algunas de las plataformas masivas de contenido y redes sociales en diversos países (China, Corea del Norte, India, Pakistán, Turquía, Egipto o Cuba, entre ellos). En Europa, sin llegar a esos límites, se han aprobado normas polémicas y tachadas de intervencionistas. Por ejemplo, la directiva europea de *copyright* promovida por los gobiernos españoles del PP y el PSOE. La norma, que supuestamente busca proteger a los autores y creadores de contenido, ha resultado ser un instrumento de vigilancia y censura.

En la práctica, se traduce en que quienes generen y carguen contenido en internet que pueda contener material protegido por derechos de autor correrán el riesgo de bloqueo, incluido aquel contenido generado por usuarios sin fines comerciales. Son también una barrera de entrada para las pequeñas plataformas, incapaces de afrontar los costes que suponen.

Las plataformas se vuelven directamente responsables del contenido subido por los usuarios, lo que deriva en la eliminación arbitraria de contenido según sus términos y condiciones. Como resultado, se legitima el bloqueo de las creaciones de muchos autores (como hemos visto con los ejemplos de los humoristas en YouTube o Instagram). Estos tienen, por tanto, menos opciones sobre dónde compartir sus creaciones. La norma ha sido criticada por estar hecha a medida de los monopolios de los derechos de propiedad intelectual, y, sin embargo, no garantiza el derecho de los autores a vivir dignamente de su trabajo.**[74]** Eso además de imponer obligaciones y limitaciones que constituyen una amenaza para la libertad de expresión y el derecho de acceso a la información de los usuarios.

La directiva de *copyright* no es la única norma cuestionable promovida en o desde España. En 2020, el Congreso aprobó la «proposición no de ley sobre la prevención de la propagación de discursos de odio en el espacio digital».**[75]** En el texto se propone, entre otras cosas, obligar a las redes sociales a «eliminar o deshabilitar de la web los contenidos que inciten al odio y a la violencia», en un plazo de veinticuatro horas, o de una hora cuando las víctimas sean menores de edad. La propuesta fue criticada por dejar en manos de las plataformas, y no de un juez, decisiones en materia de libertad de expresión.

Ese mismo año (2020), el Consejo de Seguridad Nacional (CSN) aprobó el llamado «procedimiento de actuación contra la desinformación»**[76]** que le valió al Ministerio de la Presidencia el apelativo de «Ministerio de la Verdad». La orden tiene un propósito lícito a priori: establecer mecanismos para analizar de manera continua el fenómeno de la desinformación, aumentar la transparencia sobre su origen y cómo se produce y difunde, evaluar su contenido y apoyar el fomento de la información veraz. El problema no es el qué, sino el cómo. Será el propio Gobierno el que decida qué es verdad y qué no, algo que parece más propio de países autoritarios como China que de una democracia occidental.

Resulta chocante y contradictorio, cuando menos, que, siendo los gobiernos y los partidos políticos los principales y mayores productores de desinformación, sea un Gobierno el que se encargue de controlarla. A menos que solo se pretenda controlar la desinformación que atente contra él, erigirse en juez de la verdad o incluso censurar información verídica. Muchas cuestiones quedan abiertas: ¿quién decidirá qué es real y qué no, qué se controla y comprueba y qué no, y con qué metodología? ¿Qué se define como «noticia falsa», o qué es satírico y qué no? ¿Quién ordenará la eliminación de contenidos o incluso el cierre de webs? ¿Secuestrará el Gobierno

publicaciones digitales? Son algunas de las dudas que plantea al respecto la iniciativa contra la desinformación Maldita.[77]

El caso de España no es único. Cada vez más países democráticos abren la puerta a la censura *online* con normas similares a la española. Entre ellos, Francia, Alemania, Australia o Nueva Zelanda. Como sucedía con la directiva de *copyright*, la orden contra la desinformación perjudicará a quienes menos recursos tengan y reforzará el poder de los grandes actores mediáticos —incluso de aquellos emisores de desinformación—, que podrán absorber los costes de las multas impuestas. Incluso puede desincentivar la creación de nuevas iniciativas informativas en países con estas normativas simplemente por evitar los riesgos.

Y de la censura a la autocensura. El ojo que todo lo ve en internet ejerce como instrumento de coerción personal. Los espacios de comunicación *online* están tan plagados de troles y discursos de odio como de postureo, diplomacia, ego y restricciones autoimpuestas. Ya sea por ser políticamente correctos, por el miedo a que algo se pueda tergiversar o usarse en contra de uno mismo, por aparentar, por mostrar aquello que se cree que los demás quieren ver o por enseñar solo aquello que refuerza la imagen que cada cual quiere dar, la necesidad de aceptación social condiciona lo que se publica en la plaza pública del ciberespacio. Es un ejemplo más del poder que tiene sobre las personas la anticipación de recompensas sociales de las que hemos hablado en el capítulo 4.

No ayuda a la libertad de expresión el hecho de que sea enormemente difícil borrar nuestra huella *online*. Famoso es ya el caso del español Mario Costeja, que pidió a Google eliminar de su buscador los enlaces a dos anuncios publicados en *La Vanguardia*. Eran anuncios de una subasta de inmuebles derivados de un embargo de deudas a la Seguridad Social que Costeja había contraído diez años antes y que ya no tenían vigencia.

El caso pasó por la Agencia Española de Protección de Datos (AEPD) y por la Audiencia Nacional y llegó hasta el Tribunal Europeo de Justicia en 2014. Al final, este reconoció en su sentencia[78] que el tratamiento de datos que realizan los motores de búsqueda está sometido a las normas de protección de datos de la Unión Europea y que las personas tienen derecho a solicitar, con ciertas condiciones, que los enlaces a sus datos personales no figuren en los resultados de una búsqueda en internet realizada por su nombre.[79]

Es lo que se conoce como «derecho a la supresión» o «derecho al olvido». El Tribunal Constitucional español también reconoció este derecho, en 2018, «como facultad inherente al derecho a la protección de datos personales, y por tanto como derecho fundamental».[80] Lo hizo a raíz de la demanda contra *El País* de dos personas condenadas por tráfico y consumo de drogas en la década de 1980. Su petición era que las noticias publicadas sobre su caso no pudieran asociarse a su nombre ni en dicho diario ni en búsquedas en Google.

La complejidad de los casos y el hecho de que llegaran a instancias tan altas como el Tribunal Constitucional o el Tribunal Europeo de Justicia demuestran que hacer efectivo este derecho al olvido no es un camino de rosas. Ejercerlo es relativamente sencillo, pero eso no significa que se cumpla. Desde 2014, España ha remitido a Google 76.893 peticiones de supresión de casi 250.000 direcciones web, pero el buscador ha suprimido menos del 38 por ciento de ellas.[81] Además, los usuarios no disponen de herramientas de verificación de dicha supresión y, dada la velocidad de propagación y réplica del contenido *online*, puede que los datos borrados permanezcan en otro lugar.[82]

No obstante, el derecho al olvido no es absoluto y puede chocar con otros. Por eso tiene excepciones. No se aplica si impide ejercer el derecho a la libertad de expresión e información, el cumplimiento de una obligación legal o de una misión realizada en interés público, o la formulación de reclamaciones.[83] También se puede obviar por razones de salud pública o con fines estadísticos, de archivo en interés público o de investigación científica o histórica.

El derecho a la supresión puede ser crucial para la reputación de las personas, en la vida tanto *offline* como *online*. Máxime cuando es la reputación lo que rige las relaciones en el ciberespacio. Es un hecho que no pasa desapercibido a los estados totalitarios. ¿Qué pasaría si existiera un sistema que marcase nuestro prestigio o descrédito sobre la base de cada una de nuestras actividades diarias (dentro y fuera de internet) y las registrase? ¿Un sistema capaz de condicionar nuestras acciones para que nos comportemos como se espera de nosotros? Es la idea detrás del opaco Sistema de Crédito Social (SCS) chino, aún en desarrollo.

El polémico SCS es —dicho de manera suave— el intento del Gobierno chino de modernizar su capacidad de gobernanza a través de datos y tecnología.[84] Es decir, una forma de aprovechar toda la información de los ciudadanos ya informatizada y disponible *online* para forzar a las personas a comportarse como quiere el Gobierno.

No es, como se suele contar, un sistema para calificar la moralidad de los ciudadanos al estilo de alguno de los episodios de la serie *Black Mirror*.[85] Se trata de experimentos de uso de datos públicos para mejorar la gobernanza del país de acuerdo con sus propias normas (por muy cuestionables que estas puedan ser), para que las personas se comporten de manera más honesta y conforme a los intereses del partido. Para ello, el sistema incluye sanciones y recompensas, listas negras y listas rojas para calificar a los ciudadanos. Es algo que recuerda de forma inevitable al certificado franquista de buena conducta.

La recopilación de datos para el SCS se nutre esencialmente de la información crediticia de los habitantes, pero también de cientos de portales estatales que incluyen de forma pública sanciones, licencias administrativas, propiedad de la tierra, avisos de licitación, calificación crediticia, crédito corporativo, negocios extranjeros, etc.[86] En estos portales de cara al público, las agencias estatales, el sector privado y los ciudadanos pueden consultar información y obtener otros servicios crediticios. Para

facilitar la búsqueda, a cada empresa se le asigna un código y a cada persona un número de identidad, vinculados con un registro permanente.

La combinación de la información crediticia en estas plataformas crea la capa crucial de datos del SCS. A partir de ellos se configuran las listas negras y las listas rojas, y también el régimen de sanciones y recompensas conjuntas que constituye la iniciativa clave del SCS hasta la fecha.[87] ¿Qué contienen dichas listas? Las negras, información sobre las personas o entidades que infringen las leyes, regulaciones o decisiones legalmente vinculantes. Sus nombres se pueden buscar públicamente y, en ocasiones, para vergüenza pública, se muestran en espacios públicos. Estar ahí se traduce en castigos como la imposibilidad de obtener créditos bancarios o subsidios estatales o de comprar vuelos o billetes de tren de alta velocidad.[88] Con ello se busca coaccionar a las personas o empresas para que cumplan con sus obligaciones legales. Las listas rojas, por su parte, incluyen a los ciudadanos ejemplares dentro de su jurisdicción.

Algunos gobiernos municipales de China experimentan con sistemas de puntuación de los ciudadanos según su nivel de cumplimiento de las normas y promesas de cada persona en la vida diaria.[89] Son, por el momento, voluntarios, y se accede a ellos a través de una aplicación móvil que muestra a cada persona su puntuación. Esta se calcula sobre la base de modelos similares a métodos de calificación crediticia existentes —como el FICO—, pero mezclados con un conjunto diferente de variables.

Los sistemas de puntuación se centran, hasta la fecha, en proporcionar recompensas e incentivos para quienes cuentan con puntuaciones altas.[90]Así se fomentan los comportamientos que el Gobierno chino considera deseables: actividades como el voluntariado, la donación de sangre, el uso del transporte público, la separación de residuos o trabajar en áreas de interés público. A cambio, las personas con más puntos obtienen descuentos o acceso prioritario a servicios. Aquellos con un puntaje bajo no son castigados, si bien se les niega el acceso a los beneficios otorgados a quienes tienen más puntos.

La vigilancia en China, como es bien sabido, no se reduce a este Sistema de Crédito Social. El problema, más allá del SCS, son las leyes cuyo cumplimiento quiere reforzar. Este plantea, además, serias preocupaciones sobre la privacidad. Al romper los silos de datos y vincular los datos públicos recopilados por diferentes entidades estatales y por el sector corporativo, estos sistemas aumentan el riesgo de invasión de la intimidad.

CONTROL VISUAL Y CONTROL PRIVADO, DELEGACIÓN DE PODER Y CONFLUENCIA DE TODAS LAS FORMAS DE CONTROL

De 1984 a Un mundo feliz

El SCS es una pieza más del rompecabezas de vigilancia chino. Un país tan digitalizado que el sistema de pago más usado, con diferencia (83 por ciento), son las aplicaciones móviles como WeChat Pay o Alipay.[91] Un país con cientos de millones de cámaras de vigilancia provistas de sistemas de reconocimiento facial. En un futuro cercano, toda persona que entre en un espacio público podría ser identificada instantáneamente mediante estos sistemas.[92]

La videovigilancia es vista a menudo como una herramienta que usa el Gobierno para mantener la seguridad ciudadana, no como un sistema de vigilancia de su pueblo. A esta se unen tecnologías basadas también en inteligencia artificial como el reconocimiento inteligente de sonidos. Compañías como iFlytek colaboran con las autoridades chinas en la implantación de sistemas para identificar automáticamente las voces de personas concretas en conversaciones telefónicas.

Con la excusa de velar por la seguridad de los ciudadanos, China adquiere cada vez más dominio político sobre los millones de habitantes del país. Por supuesto, esta estrategia no es exclusiva del gigante asiático. De hecho, Estados Unidos tiene, per cápita, más cámaras de circuito cerrado de televisión (CCTV) que China.[93] Londres, la capital británica, se encuentra entre las diez ciudades del mundo con una mayor cantidad de cámaras de vigilancia instaladas (el resto, excepto Nueva Delhi, son todas chinas).

Hablando de videovigilancia: en España, Renfe anunció en julio de 2020 la puesta en marcha de pruebas piloto de un sistema de análisis de imágenes de videovigilancia en andenes para detectar, en tiempo real, si se rebasaba la capacidad de aforo en los trenes de cercanías.[94] Unos meses después, en febrero de 2021, la operadora decidió que era hora de ampliar las capacidades de dicho sistema y abrió una licitación pública para el desarrollo de un *software* capaz de distinguir por origen étnico, sexo o vestimenta, como reveló *El Confidencial*.[95] La polémica hizo que Renfe retirase el pliego dos días después.

Las videocámaras son el símbolo de la vigilancia por antonomasia, mientras que otros aparatos con apariencia más inocua pasan desapercibidos. En la era de la conectividad y la inteligencia artificial, cualquier dispositivo «inteligente» es un arma de vigilancia que otorga una capacidad de control estatal sin precedentes. Las agencias de inteligencia no necesitan espiar, solo pedir a las empresas tecnológicas lo que desean.[96] Lo hacen gracias a las llamadas «puertas traseras», que permiten acceder sin impedimentos a un sistema informático o a datos cifrados.

Snowden, buen conocedor de este tipo de estrategias por parte de los gobiernos, ha denunciado en numerosas ocasiones los intentos del Gobierno estadounidense de rebajar la seguridad y el cifrado de las empresas tecnológicas de vigilancia, a cuyos datos quiere poder acceder lo más fácilmente posible sin necesidad de recurrir a la vía judicial. Conocidas son las presiones del FBI para que Apple abandonase sus planes de permitir que los usuarios del iPhone cifren completamente las copias de seguridad de sus dispositivos.[97] El Gobierno estadounidense pidió tanto a Apple como a

Facebook crear puertas traseras legales para los datos cifrados en su poder, y, ante la resistencia de ambas empresas, amenazó con hacer cumplir sus peticiones a la fuerza. **[98]**

Europa tampoco es una santa en esto. A finales de 2020, el Consejo de Ministros de Interior de la Unión Europea aprobó una resolución**[99]** para obligar a los proveedores de servicios *online* a facilitar técnicamente la posibilidad de descifrar los datos de las comunicaciones electrónicas. Es decir, empresas como Google, Facebook, Signal o Apple tendrán que introducir «puertas traseras» en sus sistemas.

En un mundo videovigilado en el que tanto empresas como gobiernos pueden acceder a nuestros datos más íntimos, la sensación de estar siendo observados es permanente. El panóptico fuerza así la conformidad, la docilidad y la autocensura constante. ¿Y si, además, ese panóptico controlador se extendiese al ámbito económico y financiero? Es algo que podríamos ver pronto, de la mano de las llamadas *govcoins*, las criptomonedas estatales. Son formalmente conocidas como Moneda Digital de Banco Central (CBDC, por sus siglas en inglés) y tienen validez legal en el país donde se emiten.

En abril de 2020, China se convirtió en la primera gran economía en poner a prueba una moneda electrónica con el lanzamiento del yuan digital. Otras sesenta y una naciones están explorando hacerlo.**[100]** España es una de ellas, en el marco del proyecto europeo del euro digital. Tanto Europa como Estados Unidos están acelerando sus planes de activación de criptodivisas para competir con China.

Las CBDC prometen combatir el blanqueo de dinero o la financiación del terrorismo, pero también centralizan el poder en el Estado y modifican la forma en que se asigna el capital. Pueden usarse como herramienta de vigilancia y control: desde rastrear las transacciones de los ciudadanos hasta cobrar multas de forma automática y sin derecho a réplica.

Sin necesidad de esperar a que eso suceda, la realidad actual transcurre ya a medio camino entre *1984*, de George Orwell, y *Un mundo feliz*, de Aldous Huxley. Un mundo que se somete de buen grado al Gran Hermano que observa, a cambio de productos y servicios que ofrecen comodidad y gratificaciones sociales, cuya existencia no es desafiada, sino alimentada. Un sistema que, en vez de a la violencia, recurre a la domesticación; que ofrece «una vida eficaz en torno a la eliminación progresiva del caos, la incertidumbre, el conflicto, la anomalía y la discordia en beneficio de la predictibilidad, la regularidad automática, la transparencia, la confluencia, la persuasión y la pacificación», como escribe Zuboff. Un porvenir de sórdida y esterilizada tiranía; una tercera modernidad que resuelva nuestros problemas a costa de nuestro futuro humano.**[101]**

Es el mundo feliz del capitalismo de la vigilancia y el colonialismo de datos. El mundo de la servidumbre y la rendición o, peor, la delegación del poder a quienes codifican los algoritmos y máquinas, en pro de la eficiencia. Un mundo donde la democracia podría llegar a verse como una forma ineficiente de tomar malas

decisiones.[102] Un mundo de ceros y unos donde se prioriza la computación como una forma superior y racional de toma de decisiones sobre la base de que los números no mienten; donde se extiende la falsa impresión de que los sistemas actuales han superado las capacidades humanas, hasta el punto de pensar que las máquinas pueden manejar mejor nuestras vidas.

Es lo que el erudito francés Alain Supiot llama «gobernar por números»: una manera de limitar el pensamiento acumulando métricas sobre métricas. Un sistema que nos condenará a perder la habilidad de pensar libremente: al confiar todo a las máquinas, perderemos nuestras facultades críticas, que solo mejoran mediante el uso continuado de la razón, la evidencia y la inquisición moral; que requieren estar alerta, consciente, ser objeto de una variedad de ideas desafiantes y pensar detenidamente sobre las influencias que acarrean.[103]

Es este un sistema tiránico que aprovecha cualquier oportunidad para aumentar su dominio y control social, su grado de autoritarismo. Lo hemos visto claramente con la pandemia de la COVID-19, que se lo ha puesto en bandeja tanto a corporaciones tecnológicas, que han aumentado sus ingresos y su poder, como a gobiernos, que han impuesto medidas represoras contra unas libertades individuales que corren el riesgo de pasar de ser excepcionales a ser permanentes. Un riesgo muy real que ya se ha materializado en lugares como Singapur, donde se animó a la población a inscribirse en el programa digital nacional de rastreo de contactos con el reclamo de que los datos solo se utilizarían para el seguimiento del virus. Ahora la inscripción es obligatoria para entrar en lugares públicos y la policía puede acceder a los datos para investigaciones criminales.[104]

Mientras algunos imponen el uso de ciertas *apps*, otros hacen que tratar de abandonarlas sea desesperante. Quienes tengan una cuenta en Amazon Prime pueden comprobarlo fácilmente. Una investigación en Europa y Estados Unidos llevada a cabo por el Consejo de Consumidores de Noruega acusó a la empresa de usar patrones oscuros para evitar que los consumidores abandonaran el servicio Prime. En concreto, mediante «características de diseño manipuladoras» que «socavan la capacidad de los consumidores para tomar decisiones libres e informadas al hacernos actuar en contra de nuestros propios intereses».[105]

A raíz del informe noruego, varias organizaciones estadounidenses pidieron a la Comisión Federal de Comercio de Estados Unidos (FTC, por sus siglas en inglés) que analizara si las prácticas de Amazon violan la ley del país. «El modelo de suscripción de Amazon Prime es como una trampa para cucarachas: entrar apenas requiere esfuerzo, pero escapar es un calvario», dicen en su carta a la FTC.[106] No exageran. Yo misma he hecho la prueba, y doy fe de que así es.

El poder de la tiranía digital choca con el anhelo de internet como poder descentralizador. La red se ha acabado centralizando a través de la influencia de unas pocas grandes corporaciones. Si las comparásemos por el número de usuarios con los países más poblados del mundo, muchas de ellas se situarían en el top 5. En él

estarían Facebook, WhatsApp, China, India e Instagram como los «países» más grandes. Y resulta que tres de ellos pertenecen a una misma empresa —Facebook— dirigida por una persona no elegida democráticamente (como no lo ha sido tampoco Xi Jinping, el presidente de China).[107]

Estas empresas pueden llegar a una inmensa cantidad de gente sin ningún tipo de rendición de cuentas. Pueden ejercer como monopolio y aplastar a sus competidores, privatizar la gobernanza y diseñar a su antojo el funcionamiento de lo *online* y las reglas de gobierno de internet.

De cómo unas pocas corporaciones han llegado a imperar en el mundo y de las promesas rotas que han arrastrado a su paso, y de qué forma el utópico mundo de la internet libre ha derivado en un sistema *online* de autoritarismo extractivo y tiranía digital hasta hacer renegar de la red de redes a algunos de sus padres creadores, hablaremos en el siguiente capítulo.

8

Promesas rotas

> *Estamos muriendo. La única cosa que vive aquí es la Máquina. Nosotros creamos la Máquina para cumplir nuestra voluntad, pero ahora que la hemos creado no podemos cumplir nuestra voluntad.*
>
> E. M. FORSTER, *La Máquina se para*

Llegamos hasta aquí tras un camino plagado de promesas rotas que han servido para aumentar el poder de quienes ya lo detentaban y para colmar las arcas de quienes ya tenían los bolsillos llenos; unas promesas que hacían vislumbrar un mundo mejor en los albores de internet y que han derivado en una realidad muy distinta. «Es disfuncional y tiene incentivos perversos»,[1] dice Tim Berners-Lee, creador en 1989 de la World Wide Web (la www, o web) y del lenguaje HTML, un hito clave en la masificación de internet.

Berners-Lee fusionó internet y el hipertexto de modo que cualquier persona pudiera utilizar un ordenador para navegar de forma sencilla, sin importar su ubicación geográfica, a través de contenidos entrelazados. Su creación nació con vocación de ser libre, gratuita y abierta, «un lienzo en el que se puedan dibujar cosas maravillosas».[2]

El pionero soñaba con una internet que proporcionase las más punteras herramientas para resolver los problemas más acuciantes y crear nuevas, mejores y más eficientes formas de democracia y de argumentación, y más y mejor transparencia y rendición de cuentas.[3] Para tratar de garantizarlo creó en 2008 la W3F Foundation. En 2019, treinta años después de crear la web, un profundamente decepcionado Berners-Lee publicó un manifiesto[4] en el que llamaba a la acción para tratar de salvarla:

> La web se ha convertido en una plaza pública, una biblioteca, un consultorio médico, una tienda, una escuela, un estudio de diseño, una oficina, un cine, un banco y mucho más. Por supuesto, con cada nueva función, cada nuevo sitio web, la división entre los que están conectados y los que no lo están aumenta, lo que hace que sea aún más imperativo que la web esté disponible para todos.
>
> Y aunque la web ha creado oportunidades, ha dado voz a los grupos marginados y ha facilitado nuestra vida diaria, también ha abierto puertas a los estafadores, ha dado voz a quienes propagan el odio y ha facilitado la comisión de todo tipo de delitos. […] es comprensible que muchas personas sientan miedo y no estén seguras de si la web es realmente una fuerza para el bien.

Las palabras de Berners-Lee esbozan las formas en las que se han transgredido los valores fundacionales de internet y de la web, y sus promesas rotas. «Internet os hará libres», «Internet será global, abierto, neutral, horizontal, meritocrático, transparente y democrático». Son cantos de sirena de lo que pudo haber sido y no fue; el anhelo de lo que tal vez nunca será.

DESIGUALDAD Y VULNERACIÓN MASIVA DE DERECHOS

> Internet no es un lujo, es una necesidad.
>
> BARACK OBAMA,
> expresidente de Estados Unidos

Los derechos humanos se ven vulnerados a diario *online*.[5] Hablamos de tecnologías conectadas que discriminan de forma injusta, clasificando erróneamente a personas por su color de piel o negándoles oportunidades sin ningún motivo que vaya más allá de sus rasgos físicos. También de sistemas que atentan contra el derecho a la dignidad en tanto que todo aquel que no forma parte de la media de la realidad algorítmica es susceptible de ser mal clasificado o no considerado por estos sistemas, lo que le obliga a expresar su no normalidad y a revelar cosas de sí que pueden ser importantes para su dignidad. De procedimientos que transgreden de forma sistemática la presunción de inocencia, recogiendo por defecto todos los datos posibles para analizar si hay en ellos algo sospechoso (contrario al Estado de derecho y que nos pone a todos bajo sospecha).

Esto desemboca en un derecho clave: el derecho a la intimidad. La privacidad no solo es importante en sí misma, sino que es un «derecho portal»: abre la puerta al ejercicio de otros derechos (como la autonomía personal, la dignidad, la no discriminación, la integración social) o al de las libertades de reunión, de asociación y de movimiento. Su incumplimiento no solo da lugar a dinámicas en que los datos se utilizan para vigilar y controlar a los pobres, sino que permite perpetuar los privilegios: fortalece las dinámicas de poder preexistentes. Por eso es tan importante.

El uso de tecnologías opacas (cuyo funcionamiento impide saber con base en qué se ha tomado un resultado determinado) o la ausencia de transparencia e información a los usuarios sobre cuándo estos sistemas se están usando conducen, además, a la incapacidad de defenderse por parte de las personas afectadas.

Estas últimas suelen ser también las más vulnerables y las que más sufren las consecuencias de la desigualdad y sus brechas. Empecemos por lo obvio: la brecha digital. Internet se ha ensalzado como una fuerza para obtener una mayor igualdad capaz de derribar barreras geográficas, económicas, raciales y de género. Pero una cosa es la capacidad y otra que esta se materialice. La pandemia de la COVID-19 lo ha puesto negro sobre blanco: no solo ha generado más dependencia a estar conectados, sino más desigualdad entre quienes tienen y quienes no tienen acceso a

una conexión decente o a un dispositivo para conectarse, y entre quienes disponen o no disponen de conocimientos para usar los recursos que lo *online* ofrece.

«Desde que inventé la web, todos los años ha aumentado su importancia en la vida de las personas, pero al mismo tiempo también ha crecido la privación de derechos de quienes no pueden conectarse. La COVID-19 ha sobrealimentado este proceso. La web es un salvavidas en esta crisis y, sin embargo, es un salvavidas que se les niega a miles de millones de personas justo cuando más lo necesitan», dice Berners-Lee.

Cuando internet se convierte en la principal o única fuente de acceso a la educación, el trabajo, la información o el entretenimiento, los efectos de la exclusión se multiplican y emergen las desigualdades. A estas les hemos puesto rostro durante la crisis del coronavirus: esos niños que no han tenido acceso a las clases *online*. Esos pequeños a los que se les ha negado la posibilidad de seguir aprendiendo como lo hacen sus compañeros representan la brecha digital, similar a la de sus padres y sus mayores.

Aún en el siglo XXI, casi la mitad de la población mundial está desconectada de internet.**[6]** Solo un 19 por ciento de los habitantes en países en desarrollo tiene acceso a una conexión, en comparación con el 87 por ciento en países desarrollados.**[7]** Sin embargo, incluso en estos últimos la brecha digital persiste. En España, trece millones de personas carecen de cobertura de internet apropiada.**[8]** Se concentran en la llamada «España vaciada»: casi veintisiete mil poblaciones con menos de diez habitantes. Esto en un país puntero en infraestructuras de telecomunicaciones, donde el 99,5 por ciento de la población puede conectarse a la banda ancha móvil 4G.

Pero el acceso no lo es todo. Incluso para muchas de esas personas con una conexión a internet apropiada sigue habiendo un problema de base: una falta de preparación para usar las ya no tan nuevas tecnologías. Más del 40 por ciento de la población española carece de habilidades digitales básicas, a pesar de que la mayoría de los trabajos las requieren.**[9]**

La brecha digital se agrava por género (es mayor en el caso de las mujeres), edad (mayor entre la gente de edad más avanzada), territorio (mayor en poblaciones más pequeñas), nivel de renta (mayor para los más pobres) y nivel de estudios (mayor para las personas con menos formación).**[10]** El 60 por ciento de quienes superan los ochenta años reconoce dificultades para comunicarse a través del móvil.**[11]**

Las diferentes capacidades también influyen; ciertas discapacidades aumentan la brecha digital. El extremo de la brecha digital lo representaría una mujer mayor sin empleo, con bajos ingresos, con poca formación y habitante de una zona rural.**[12]** En ella se encarna no solo la desconexión digital, sino también, y de forma generalizada, la exclusión social.**[13]**

Las diferencias de acceso, calidad de conectividad y preparación para su aprovechamiento refuerzan formas previas de desigualdad. Y no solo eso, pues amenazan el progreso mundial, especialmente en convergencia con otro peligro: una

pandemia como la que comenzó en 2019 con la COVID-19. Esta no nos ha igualado, sino que ha magnificado las desigualdades. Frente a ello está la reivindicación del acceso a internet como derecho humano, que lideran el propio Berners-Lee y otros muchos grupos activistas de los derechos digitales como Xnet, encabezado por la dramaturga italiana Simona Levi.

DISCRIMINACIÓN *BROGRAMMER*

La falta de acceso a internet explica en buena parte la brecha de género en las capacidades digitales y tecnológicas. La asequibilidad de la tecnología y la falta de habilidades relevantes en el uso de herramientas digitales son dos de las principales razones.[14] En 2018 había unos doscientos cincuenta millones menos de usuarias de internet que de usuarios.[15] En 2019, la brecha de género en términos de presencia *online* era del 17 por ciento,[16] y en 2020 los hombres seguían siendo un 21 por ciento más proclives a estar *online*.[17] Además, en comparación con estos, hay doscientos millones de mujeres menos entre quienes poseen un teléfono móvil.[18]

La otra gran barrera en la brecha de género digital y tecnológica es sociocultural y de estereotipos: entornos que desde el primer momento no dieron la bienvenida a las mujeres; una cultura hostil a éstas forjada entre profesionales de la tecnología masculinos en entornos agresivos con una alta competitividad y amiguismos. De ahí nació el término despectivo *brogrammers*, combinación de *brothers* y *programmers* («hermanos» y «programadores»). Hace referencia a la hermandad y al «colegueo» del colectivo de informáticos masculinos aún vigente; una cultura machista que sigue expulsando a las mujeres del sector tecnológico a través de formas encubiertas de sexismo y de los mal llamados (y a menudo denunciados) «micromachismos».[19]

Esta realidad es anterior a internet, pero se trasladó también a la red de redes. Como comenta la presidenta de Wikimedia Foundation, María Sefidari, la desproporción entre hombres y mujeres *online* es un problema desde los comienzos de internet.[20] «Era el internet de ellos. La propia Wikipedia nació dominada por los hombres. Veíamos el potencial de la red, pero también las barreras para las mujeres. Un hostigamiento sin precedentes para intentar silenciar y apartar nuestras voces. El ideal de internet utópico no se veía como tal para la mitad de la población», asegura Sefidari.[21]

La experta habla de la llamada «misoginia en red», una forma de activismo misógino *online* que usa internet para apartar a las mujeres. A través de diferentes canales *online* crean y expanden lo que la profesora Adrienne Massanari llama «tecnoculturas tóxicas»,[22] mediante tácticas de acoso implícito o explícito. Massanari denuncia en una de sus investigaciones que la plataforma social Reddit se ha convertido en un centro para este tipo de acción. Sostiene que el propio diseño de Reddit, el algoritmo y su política de funcionamiento y norma apoyan implícitamente este tipo de culturas y les proporcionan un terreno fértil. Como ejemplo pone el

Celebgate y el Gamergate.[23] El primero se refiere al evento sucedido en agosto de 2014 con la publicación *online* de centenares de fotografías íntimas y desnudos de famosas en la web 4Chan. Estos corrieron como la pólvora a través de Reddit y otras plataformas como Tumblr. Ese mismo mes comenzó el Gamergate, también en 4Chan y Reddit. Se trata —como explica el investigador Víctor Navarro— de un movimiento supuestamente dirigido contra la corrupción en la prensa especializada en videojuegos que, en realidad, trataba de bloquear la entrada de ideas progresistas y feministas en la industria.[24]

Son solo algunos ejemplos de cómo los grupos misóginos se organizan a través de las plataformas *online*. Si bien la Web 2.0 ha proporcionado a todos —hombres y mujeres— oportunidades sin precedentes para relacionarse y comunicar, acceder, producir y distribuir información, y es una fuente de placer, creatividad y colaboración, hay un alto nivel de hostigamiento claramente enraizado en el sistema de género. Lo constata la académica Laura Favaro tras un profuso análisis de género de la literatura científica en el campo de los «estudios de internet». Escribe Favaro que la misoginia en red está cada vez más dirigida hacia todas las usuarias, y que «los usos feministas de internet coexisten con una fuerte resistencia misógina, al igual que con una web altamente comercializada y profundamente cimentada en posicionar a las mujeres como sujetos a la vez que objetos de consumo».[25]

NEUTRALIDAD *VS.* CLASISMO *ONLINE*

Un internet clasista, de dos velocidades. Es lo que permite la supresión del principio de la «neutralidad de la red» en Estados Unidos. Ni las peticiones de retraso de la votación por parte de casi una veintena de fiscales, ni las decenas de cartas de senadores, ni las encuestas en contra, ni las manifestaciones de ONG y activistas, ni los ruegos de los pioneros de internet y de las grandes compañías tecnológicas pudieron evitar que la Comisión Federal de Comunicaciones de Estados Unidos (FCC, por sus siglas en inglés) derogase —en diciembre de 2017— las normas de neutralidad de la red de 2015.

¿Qué tiene de malo? ¿En qué consiste este principio? Básicamente, establece que todo el tráfico de internet debe tratarse por igual. Es decir, las operadoras que facilitan el acceso a internet no pueden fijar diferentes tarifas ni tratar de forma distinta el flujo de datos de quienes proveen servicios y/o contenido a través de sus redes (ya sea un blog, una web de venta *online*, una plataforma de música o contenido audiovisual bajo demanda, etc.). La cuestión de fondo es la consideración de internet como un derecho universal, un bien común, y no como un negocio.

La eliminación de este principio en Estados Unidos podría traducirse en la práctica en restricciones de acceso, de calidad o de velocidad a los proveedores y a los usuarios que quieran acceder a sus plataformas, aplicaciones o sitios web. Es algo que, por el momento, no ha pasado. La derogación de la norma se hizo efectiva en

junio de 2018, tras meses de litigios y de demandas en contra. Sin embargo, muchos estados decidieron crear sus propias normas de neutralidad de la red y muchos grandes operadores proveedores de servicios se comprometieron a no bloquear ni discriminar el tráfico.

Eso no significa que no vaya a pasar en un futuro, dado que la ley les permite hacerlo. Si se producen cambios, estos probablemente irán en aumento. Se materializarán poco a poco a lo largo de varios años hasta que, de repente, nos encontraremos con una internet para ricos y otra para pobres, que segmentaría entre ganadores y perdedores digitales. Las compañías podrían crear carriles rápidos por los que cobrarían (cual autopistas) un extra a los proveedores, si bien también podrían crear carriles lentos que costarían menos. Ello permitiría a cada persona decidir por qué paga. Esto está bien en teoría, pero, si no se baja el precio a los carriles lentos y se sube el de los rápidos, el resultado es que el consumidor se ve obligado a pagar más por el mismo servicio.

«Hablan de las oportunidades de que más personas puedan conectarse, pero ¿para qué si solo se les permite ver las películas que los proveedores decidan?», dijo Berners-Lee[26] en su posicionamiento sobre la derogación del principio de neutralidad de internet en Estados Unidos. Cuando él inventó la web no tuvo que pedirle permiso a nadie, y así debe seguir siendo. Máxime en un mundo en el que las empresas no pueden operar sin internet, cuyo acceso controlan unos pocos proveedores.

Acabar con la neutralidad de la red es poner barreras a la creatividad, a la innovación y a la libre expresión *online*. Es un ataque directo a uno de los pilares de internet. La ofensa es tal que, ante la derogación de este principio en Estados Unidos, doscientos pioneros de internet enviaron una carta[27] a favor del restablecimiento de la libertad en internet al Gobierno estadounidense, al que acusaron de tener una comprensión defectuosa y objetivamente inexacta de la tecnología de la red.

Otro frente que también sufre con el debilitamiento del principio de neutralidad *online* es el científico. La revista *Nature*[28] advierte de que la pérdida de neutralidad de la red podría afectar negativamente a la investigación. También que una internet de varias velocidades podría conducir a la ciencia al carril lento. En él podrían quedar atrapados grandes volúmenes de datos enviados desde América Latina hacia Europa, como los que salen de los telescopios de Chile, ya que su ruta pasa por Estados Unidos.

Las universidades y los estudiantes, especialmente en los países más pobres, podrían enfrentarse a tarifas prohibitivas de acceso y descarga. La amenaza afecta también a la difusión de las publicaciones académicas. Y también podría suponer un gran paso atrás en los avances hacia una ciencia abierta propiciados por internet, que no deja de ser —además— una herramienta científica.

¿Cómo afecta todo esto a Europa y a España? Vivimos en un mundo globalizado y permeable a la onda expansiva de Estados Unidos. Si un país que se vanagloria del

internet abierto toma este tipo de medidas, ¿por qué no iban otros a sentirse legitimados para hacer lo propio? En Europa está vigente la ley de neutralidad de la red aprobada en 2015 por el Parlamento y la Comisión Europea. Una norma que tiene algunas lagunas. En países como Portugal hay operadoras que, para aventajar a la competencia, no cobran datos por usar ciertas aplicaciones o servicios como WhatsApp, Instagram o Spotify (lo que, además, refuerza el poder de estas plataformas y aplicaciones). En Suecia, la empresa de telecomunicaciones Telia Company también sigue esta práctica de «tipo cero» (*zero rating*).

Desde que entraron en vigor las reglas de neutralidad de la red de Europa, esta clase de práctica se ha extendido a veinticinco de los veintisiete países de la Unión Europea[29] (a todos menos a Bélgica y a Finlandia). En algunos, la diferencia de coste entre las aplicaciones con precios especiales y el resto de internet se ha multiplicado por setenta.[30] En España se considera que la neutralidad de la red disfruta de una calidad mediocre.

Las opciones para los usuarios finales están restringidas, mientras que cada vez más empresas crean sus «jardines amurallados» *online*, en los que no se puede entrar sin suscripción. Al tiempo, el mercado único digital de Europa se ha visto fragmentado por las nuevas barreras de entrada al mercado que han creado las empresas de telecomunicaciones. A pesar de las directrices que exigen que estas empresas proporcionen al menos un nivel mínimo de transparencia en las velocidades de internet, las operadoras no están publicando esa información y los reguladores están haciendo la vista gorda.

La ley europea de neutralidad se viola a veces impunemente, con multas que en algunos países no van más allá de los cuatro dígitos. En otros ascienden a los ocho ceros, o a los seis en el caso de España (con penalizaciones de hasta dos millones de euros). En dos países directamente no hay multas. Es el caso de Portugal e Irlanda. Este último ocupó en 2019 la presidencia del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (BEREC, por sus siglas en inglés) a cargo de la reforma de la neutralidad de la red, y en 2020 seguía manteniendo una de sus vicepresidencias.

Por otra parte, permitir que los proveedores de contenidos dominantes paguen más por un mejor acceso a los consumidores reduciría la competencia y las posibilidades de elección en todo el mundo, no solo en Estados Unidos. Los gigantes de internet —incluidas las plataformas de entretenimiento— necesitan una masa crítica de usuarios para ser económicamente viables. Cuanto más crece dicha masa crítica, más difícil es para sus competidores alcanzarla. Entre las veinte aplicaciones principales que se benefician de prácticas de «tipo cero», solo tres son de Europa. Es decir, el mercado único digital europeo sufre las violaciones de la neutralidad de la red.

Si fuera por el mundo empresarial, internet no existiría.

ANDREU VEÀ, pionero de internet

En efecto, el predominio en el mercado de unos pocos actores es tan grande que impide a otros competir. Esos actores son las GAFAM: Google, Amazon, Facebook, Apple y Microsoft. Son las empresas de internet más grandes del mundo. Juntos, los cinco gigantes tecnológicos representan un valor de mercado de más de cuatro billones de dólares[31] y cuentan, cada uno, con bases de usuarios de miles de millones de personas.

Sus equivalentes en China son los BAT o MAT: Baidu (equivalente a Google) y Meituan (reparto a domicilio) se turnan en el tercer puesto del triunvirato, que integran también Alibaba y Tencent. Juntas suman una valoración de más de un billón de dólares. La pandemia no impidió que siguieran creciendo, salvo periodos de caída para Alibaba por cuestiones políticas.

Como con las anteriores, la crisis de la COVID-19 no hizo de menos a las GAFAM, sino de más. Los ingresos de todas ellas aumentaron en 2020.[32] Amazon subió un 38 por ciento, Facebook un 22 por ciento, Microsoft un 18 por ciento, Google un 13 por ciento y Apple un 10 por ciento. Esto se tradujo en cifras récord para Amazon,[33] Google[34] y Apple.[35] La capitalización de mercado combinada de las diez empresas digitales más grandes del mundo aumentó en tres mil novecientos millones de dólares, más que el valor de todo el mercado de valores británico.[36]

Por si ya tenían poco poder, ahora tienen más. La pandemia llegó para cambiarlo todo, pero una cosa permanece igual: las empresas tecnológicas siguen imprimiendo dinero en cantidades incomprensibles. No por casualidad, sus fundadores se encuentran entre las diez personas más ricas del mundo: Jeff Bezos (Amazon) encabeza la lista,[37] Bill Gates (Microsoft) es el tercero, Mark Zuckerberg (Facebook) ocupa la quinta posición y Larry Page (Google) la octava. Entre los veinticinco más ricos están también los fundadores de Tencent (Pony Ma) y de Alibaba (Jack Ma).

Otros gigantes algo menos grandes que los anteriores, como Netflix, tampoco tienen de qué quejarse. La plataforma de contenido audiovisual bajo demanda superó sus propias expectativas en 2020 con un aumento del 31 por ciento con respecto a 2019. Ganó un total de treinta y siete millones de nuevos suscriptores.[38] Solo en el primer trimestre de 2020 Netflix duplicó beneficios y millones de usuarios.[39] No es de extrañar, dado que por esas fechas la COVID-19 confinó al mundo en casa, y el entretenimiento, las compras, el trabajo, la educación y prácticamente todo, menos hacer pan y bizcochos o sacar a pasear al perro, se trasladaron a internet.

No es que no se lo hayan ganado por méritos propios. Todas ellas son empresas disruptoras. Han sabido ver un nicho en el mercado, una necesidad no cubierta, un problema abierto o una oportunidad de negocio, y lo han resuelto de forma

tremendamente exitosa. Por eso están donde están. Y la exponencialidad y escalabilidad de internet han ayudado a ello.

Estas empresas cuentan con la ventaja del «efecto de red»: cuantos más usuarios tiene un producto, servicio, plataforma o *app*, más aumenta su valor para otros usuarios o para todos los usuarios, o les ofrece beneficios cada vez mayores. Por ejemplo, Facebook se vuelve más útil cuantos más amigos tenemos en la plataforma, los mensajes en Twitter tienen un mayor impacto potencial cuantos más usuarios haya en la red social y más personas nos sigan, y Uber es más eficiente cuantos más conductores tiene, lo cual hace posible que lo usen más usuarios, y ello aumenta la demanda de conductores, y así sucesivamente en un círculo virtuoso infinito.

Hay efectos de red directos e indirectos. En el primer caso, un aumento en el uso o los usuarios conduce a un crecimiento directo del valor para otros usuarios, como sucede con Facebook. En el segundo, es un aumento de la utilización de un servicio complementario lo que propicia un incremento del valor de los usuarios del otro lado o lados de la plataforma, es decir, del valor de la plataforma como tal. En el caso de Apple o Microsoft, por ejemplo, cuanto más usa la gente sus dispositivos o sistemas operativos, más desarrolladores crean productos pensados para ellos, lo que a su vez atrae a más usuarios.

Hay también plataformas de uno o más lados. Google es un maestro en esto: ofrece múltiples servicios complementarios —buscador, publicidad en los resultados de búsqueda, servicio de correo electrónico, almacenamiento en la nube (*online*), etcétera— que facilitan el efecto inercia de los usuarios ante el poder de una marca conocida y la capacidad de esta de aprender de ellos. La experiencia dice que, una vez que los usuarios y anunciantes se han familiarizado con los servicios de Google, son menos proclives a usar los mismos servicios de otras marcas. Es muy poco probable que una persona que lleva un año utilizando Gmail empiece a usar otro servidor. Además, se genera toda una industria alrededor del líder del mercado que refuerza aún más los efectos de red.

Mientras que Apple o Microsoft atrapan poniendo murallas, Google o Amazon lo hacen a través de esos servicios complementarios. Su forma de captar más usuarios no es la coerción, sino la apropiación o concentración. Para sus usuarios, o para los de plataformas bajo demanda como Uber, es muy fácil usar otras alternativas: solo necesitan un clic o, como mucho, un sencillo registro. El coste de cambio es mínimo o nulo, ya que el mercado cuenta con competidores igualmente accesibles. Ante la posibilidad de «multiconexión» (que los usuarios utilicen varios proveedores o plataformas al mismo tiempo), crean servicios adicionales, los adquieren, o absorben a sus competidores. Compran empresas emergentes que pueden quitarles usuarios o cuyos productos o servicios pueden ayudarles a retenerlos.

Esto no es así con redes sociales como Facebook. Si bien no cuesta dinero usar alternativas, el precio que hay que pagar es dejar de ser parte de la conversación, no estar donde están tus amigos y contactos. ¿Y de qué sirve tener presencia en una red

social que de social tiene poco o nada? O, más allá, si Facebook o Twitter son de verdad la nueva plaza del pueblo, entonces el coste del cambio es no poder entrar ni tener voz en ella.

Sea por un motivo u otro, llegamos a un resultado similar: gigantes que ejercen prácticamente como monopolios. No solo tienen una clara posición de dominio, sino que sus efectos de red, económicamente positivos en un principio, crean barreras de entrada: cuantos más consumidores y vendedores utilizan un mercado, más difícil se vuelve para un rival atraerlos. Cuanto más grandes son, más capacidad económica, de despliegue de red, etc. tienen, esto es, más matan a los pequeños competidores Ese internet abierto, colaborativo, descentralizado, horizontal y meritocrático que, por un tiempo, se vislumbró en sus albores ha cambiado. «Si fuera por el mundo empresarial, internet no existiría», dice Andreu Veà, pionero de internet.**[40]** En efecto, internet, en su concepción original, no había nacido como iniciativa empresarial. Ese es, paradójicamente, el pecado original de internet: que no incorporaba un sistema de pago en el navegador; una manera de monetizar, de hacer negocio, de gastar dinero. Lo dice Marc Andreessen, creador del primer navegador comercial, Netscape.

Esa es la razón por la que ahora el modelo de negocio *online* se basa predominantemente en la publicidad. Un modelo explotado por los gigantes que hoy dominan la red, que tratan de obtener rédito económico de todas las actividades humanas comercializables *online*. Un modelo extractivo que es la causa de las principales preocupaciones sobre la red de redes: la vigilancia y el rastreo permanente, la invasión de la intimidad y la pérdida de la privacidad, la recopilación y venta de datos de los usuarios a terceros, la asimetría de información y de poder, la desalineación de incentivos o la adicción y la necesidad de estar conectados.

Atrás quedaron los primeros años de la internet entre pares. Ahora tanto el funcionamiento como la arquitectura tradicional de internet están determinados por la concentración y la consolidación del tráfico en la red; por su centralización. Las fusiones y las adquisiciones han eliminado competidores entre operadores, prestadores de servicios, proveedores de dominios e infraestructura y desarrolladores de aplicaciones y plataformas web (que se construyen sobre la Web pública, pero que dependen, en su mayoría, de unos pocos sistemas propietarios).

Los operadores de tránsito de larga distancia son cada vez menos, pero más grandes. Afectan a servicios que históricamente se operaron de forma distribuida, como el transporte de correo electrónico o el DNS. Esto se traduce en que la mayoría de los dominios comercialmente importantes en internet están en manos de un pequeño número de grandes proveedores.

EL IMPERIO CONTRAATACA: LUCHAS DE PODER, DIVISIÓN Y *SPLINTERNET*

Esta consolidación es natural: todas las empresas quieren tener más cuotas de mercado. Lo que no es admisible es aplastar a la competencia de forma ilegal. Es la razón por la que el mismísimo Gobierno de Estados Unidos, en una jugada histórica, demandó a Facebook. Acusa a la red social de comprar rivales como Instagram o WhatsApp, «utilizando su dominio y poder de monopolio para destruir a competidores más pequeños, a expensas de los usuarios», según la fiscal general de Nueva York Letitia James.[41] Una denuncia que fue desestimada en junio de 2021 por falta de documentación.

Google, por supuesto, tampoco se libra. Igualmente significativa es la denuncia del Gobierno estadounidense al buscador por monopolio ilegal de las búsquedas y de la publicidad en estas, por excluir a sus rivales mediante tácticas como pagar para garantizar que el buscador de Google tenga una posición destacada en los *smartphones*. Algo que, por otra parte, se sabe desde hace años. De hecho, la Comisión Europea ya impuso en 2018 a Google una multa de más de cuatro mil millones de euros[42] por este tipo de prácticas para mantener el dominio en dispositivos Android.

Amazon también ha sido acusada de capitalizar el interés en productos de la competencia (limitando la capacidad de esta para promocionar dispositivos como altavoces inteligentes similares a Amazon Echo) y de no permitir que sus rivales más fuertes hagan lo mismo. Y tanto Apple como Google han sido denunciadas —y están siendo investigadas— por conductas anticompetitivas con respecto a las reglas que imponen a los desarrolladores de aplicaciones para ofrecer sus productos en las tiendas digitales de los dispositivos iOS y Android. Los términos y condiciones incluyen compartir ciertos datos con Apple y Google y darles un porcentaje de sus ventas a través de dichas tiendas. Empresas como Epic Games ya las han denunciado por abusar de su posición dominante.[43]

En China, el Gobierno investiga si el gigante de comercio electrónico Alibaba ha incurrido en prácticas monopolísticas y de abuso de su posición dominante, como, por ejemplo, limitar a los proveedores la venta de productos en otras plataformas. Algo, cuando menos, sorprendente, dado que hasta ahora las autoridades chinas habían mirado hacia otro lado, mientras este y otros gigantes tecnológicos chinos seguían creciendo. Curiosamente, la investigación se inició poco después de que el fundador de Alibaba, Jack Ma, criticara en público a los organismos financieros y a los bancos del país asiático.

Sea como fuere, el que compañías cada vez más grandes acaparen el mercado multiplica a su vez las vulnerabilidades frente a posibles ciberataques. También frente a ataques físicos: la mayor parte de los cables submarinos de fibra óptica están en manos de compañías privadas. ¿Qué pasaría si se produjese un ataque a esos cables? No es algo improbable. Hay submarinos específicamente diseñados para cortar este tipo de cableado.[44] ¿Cómo velan las compañías propietarias por su seguridad? Google tiene muy clara la parte de apropiarse de los datos íntimos de los usuarios,

pero la provisión de seguridad no está escrita en ningún sitio. No hay ninguna garantía jurídica de que eso se vaya a cumplir. Es una responsabilidad que normalmente se atribuye al Estado, al que usan como escudo cuando les interesa o al que pretenden suplantar cuando así les conviene.

«Concentración» se traduce en vulnerabilidad y también en dependencia. Si bien Europa —y especialmente España— cuenta con una buena infraestructura de telecomunicaciones y fibra óptica,[45] carece de una infraestructura competitiva para el almacenamiento de datos. Esto significa que nuestros datos, los que se generan en Europa, se alojan en servidores de fuera del Viejo Continente. La mayoría (un 92 por ciento) está en Estados Unidos.[46]

Teniendo en cuenta que los datos son el activo clave de la economía conectada, no parece buena idea mantener la subordinación. Sin embargo, el precio que habría que pagar por la independencia sería elevado; se calcula que la soberanía digital europea costaría quinientos treinta mil millones de euros.[47] La alta fragmentación del mercado europeo no ayuda a su posición frente a Estados Unidos o China. Estos tienen, además, la ventaja del primer movimiento: han invertido desde hace tiempo ingentes cantidades en su red de servidores y centros de datos.

El ideal de una internet caracterizada por el libre flujo de los datos se desvanece en un contexto en el que estos son valorados como «el nuevo petróleo» y en el que los gobiernos erigen fronteras para su circulación. Es un proteccionismo digital que convierte a la soberanía digital en algo crucial y que lleva un paso más allá la balcanización de internet. Esa fragmentación de la red de redes o *splinternet* derriba el mito fundacional de internet como red global que se muestra igual a cualquier persona sin importar dónde se encuentre. Una utopía que comenzó a desmoronarse en el momento en que ciertos países decidieron separar a sus usuarios de internet de los de otras partes del mundo. El primero de ellos fue China, que en 1997 inició la construcción de su cortafuegos *online*: su «Gran Muralla digital».

La utopía se aleja cada vez más, a medida que se intensifica la guerra comercial entre Estados Unidos y China, entre acusaciones de espionaje y bloqueo mutuo de empresas (al que Estados Unidos intenta arrastrar a Europa y al que ya se ha unido India con la prohibición de decenas de *apps* chinas). Murallas y más murallas que se levantan también en Occidente, debido a las distintas leyes de privacidad que rigen a un lado y otro del charco. Unas normas —como, por ejemplo, el Reglamento General de Protección de Datos europeo (RGPD)— que han hecho a algunas compañías estadounidenses decantarse por bloquear a los usuarios europeos para no tener que cumplirlas.

Estos movimientos reflejan cómo los gobiernos están luchando contra el mito de la internet global para volver a poner al Estado nación en el centro del poder. No se trata solo de regulación, sino que implican a infraestructuras críticas y al propio ejército. Internet se militariza. Se convierte en campo de batalla para la ciberguerra y en escenario de la llamada «nueva Guerra Fría». En él, Rusia se prepara para una

desconexión voluntaria o forzada (por un ciberataque) de internet. En diciembre de 2019 concluyó con éxito su primera prueba: logró desenchufarse de la red global, o eso dijo el Ministerio de Telecomunicaciones ruso. Su objetivo con esa prueba era comprobar el funcionamiento de la intranet rusa —RuNet— redireccionando el tráfico *online* internamente.

De funcionar, hablaríamos de la intranet más gigantesca existente y sin precedentes. Todo un sistema de internet alternativo, amurallado y controlado por el Gobierno, con capacidad para decidir a qué pueden o no acceder sus ciudadanos. Para hacerlo posible, el Parlamento ruso aprobó una ley que regula cómo se mueve el tráfico de internet, con una nueva tecnología de enrutamiento y filtrado que permite una gestión centralizada y otorga poder a la autoridad para monitorear y censurar directamente el contenido que consideren objetable. A esto se añade su intención de crear un sistema propio de nombres de dominio. Con todo ello en funcionamiento, el tráfico no tendría que entrar ni salir de las fronteras rusas.

Una internet cerrada como esta (a la que ya no se podría llamar «internet») beneficiaría a las grandes empresas rusas de tecnología. Por ejemplo, al buscador Yandex, segundo en cuota de mercado en Rusia, por detrás de Google,[48] o al proveedor de correo electrónico Mail.ru. De hecho, Rusia planea limitar la propiedad extranjera en sus empresas de internet para asegurar su control. Su Parlamento también ha aprobado un proyecto de ley que prohíbe vender *smartphones* que no tengan *software* ruso preinstalado. Incluso ha anunciado la creación de su propia Wikipedia.

EL NUEVO ORDEN MUNDIAL

Rusia, la otrora competidora de Estados Unidos en la cúspide de la carrera espacial mundial, se ve ahora eclipsada por China en la carrera de la inteligencia artificial (IA). La IA es una cosa e internet otra, pero probablemente no hablaríamos hoy de la eclosión de la primera sin la segunda, sin acceso a los datos que las compañías tecnológicas recopilan y que mejoran el funcionamiento de sus brazos ejecutores: los algoritmos.

La IA también lleva internet un paso más allá, al eliminar parte de la fricción entre los mundos *online* y *offline*. Antes la conectividad estaba necesariamente mediada por una pantalla. Ahora las capacidades perceptuales de la IA —como la visión artificial o el reconocimiento de voz— hacen que sea posible prescindir de ella, tan solo escuchando nuestra voz u observando nuestro rostro. Es lo que KaiFu Lee denomina entornos mixtos OMO[49] (*online-merge-offline*), donde lo desconectado se funde con lo conectado.

Aquí de nuevo Europa llega con retraso; depende de terceros y carece de soberanía en inteligencia artificial. El atraso general europeo en materia de digitalización alimenta los temores de que el Viejo Continente se quede obsoleto en el

nuevo orden digital mundial, uno en el que la Europa del siglo XXI podría volverse la China del siglo XIX, que pasó de ser la mayor potencia económica a un país en vías de desarrollo.

El desequilibrio geográfico de la economía digital seguirá aumentando la desigualdad entre países, y hay quienes vaticinan que, si Europa no reacciona pronto, se convertirá en una colonia digital. ¿Hay alternativa? ¿Qué nos depara el futuro? ¿Estamos a tiempo de cambiar el curso de los acontecimientos y las derivas criminales, tiránicas, autoritarias, adictivas, discriminatorias y polarizadoras de la red y las nuevas tecnologías o estas seguirán de forma inevitable su supuestamente imparable rumbo? Las respuestas no son simples y en ellas nos adentramos —con esperanza, confianza y convicción— en la tercera y última parte de este libro.

Tercera parte

Nuevo amanecer

9

Futuro incierto

¡Exigimos áreas rígidamente definidas de duda y de incertidumbre!

DOUGLAS ADAMS, *Guía del autoestopista galáctico*

¿Qué podría ser mejor? En 2015, cuando Google se reestructuró en Alphabet, su cofundador (el multimillonario Larry Page) publicó una carta abierta a internet[1] en la que anunciaba eufóricamente su visión de futuro y sus intenciones para la compañía. Tras destacar numerosas ventajas que, desde su percepción, estaban por venir, terminó el texto con una pregunta retórica: «¿Qué podría ser mejor?». La respuesta para Page era obvia: ¡nada podría ser mejor! Desde su limitada visión «googlecéntrica», el panorama era inmejorable.

Más allá del ombligo de Google, fuera de la realidad paralela en la que Page y otros líderes de la deriva monopolística y centralizadora de internet viven, la frase ya chirriaba. Hoy el quejido es atronador. Nos plantamos a comienzos del siglo XXI con una acumulación de promesas rotas que no han liberado internet de la desigualdad, el crimen, la tiranía, la adicción, la discriminación y la radicalización. El impacto de todo ello amenaza a la gobernanza pública, socava no solo la democracia, sino también la cohesión social, y acelera el colapso del medio ambiente.

PRIVATIZAR LA GOBERNANZA

¿Pagaría alguien impuestos de forma voluntaria? Tal vez alguien sí. La mayoría no. Lo mismo sucede con la autorregulación de las grandes empresas tecnológicas: no funciona.[2] Las grandes tecnológicas se unieron en 2016 en el consorcio Partnership on AI cuya misión es, en teoría, estudiar y formular las mejores prácticas en tecnologías de inteligencia artificial. La iniciativa ha sido acusada de actuar en la práctica como un *lobby* en busca de normas —o ausencia de ellas— que beneficien a sus intereses; una forma de autorregularse sin someterse al escrutinio y el voto de la gente. Dan la impresión de posicionarse en el lado correcto, cuando sus acciones no van más allá de las relaciones públicas.

Es el «teatro de ética» de la industria tecnológica: un intento de lavado de cara mediante la invocación de la ética. A Google el tema le ha sacado los colores en más de una ocasión. Por ejemplo, con la polémica cancelación de su Comité Asesor de Ética una semana después de crearlo, tras conocerse la identidad de algunos

controvertidos miembros. Mientras, el CEO de Google, Sundar Pichai, presume de los principios de privacidad en el desarrollo y uso de sus tecnologías. Los mismos principios que han llevado a su empresa a compartir sin permiso datos de usuarios de centenares de aplicaciones de Android con Facebook. Los mismos principios que les han permitido vender las búsquedas más íntimas de sus usuarios a terceros.

¿Cómo confiar en estas empresas solo porque digan que se comprometen a ser éticas o responsables, mientras miran para otro lado y hacen lo contrario? Hechos son amores, y no buenas razones. Y los hechos muestran cómo los todopoderosos de internet se comportan a menudo como gángsteres digitales al considerar que están por delante y más allá de la ley.[3]

De nuevo surgen paralelismos con la crisis financiera de 2008, cuando se permitió que una industria carente de regulación y sin control sobre sus excesos llevara a la quiebra a la economía global. Los riesgos van más allá del plano económico. Los gigantes de internet tienen poder de gobernanza para marcar las reglas del juego *online*, dictando decisiones sobre nuestra vida e imponiendo sus leyes.

El Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio, que busca regular el entorno digital, anunciado por Emmanuel Macron y respaldado por cincuenta países diferentes, incluye a compañías como Microsoft, Google o Samsung. Estas empresas tienen derecho —y es su deber— a participar en las discusiones sobre cómo fomentar la innovación o luchar contra el discurso del odio, la manipulación o el pirateo. Pero la línea entre tener voz en ellas y dictar, *de facto*, las leyes se hace cada vez más fina. Está muy bien que las empresas actúen de manera responsable, pero otra cosa diferente es que asuman la gobernanza transfronteriza y la responsabilidad de crear normas a escala mundial que atentan contra el Estado de derecho.

Son cada vez más las voces que alertan del riesgo de que el sector privado capte el interés público y de que las normas se hagan sin transparencia, sin responsabilidad y sin el mandato de la gente. Es la privatización de la gobernanza, en contraposición con un sistema de gobernanza democrática cuyo desarrollo de normas incluye a las múltiples partes interesadas.

Las GAFAM, BAT[4] y demás gigantes no solo pueden abusar de su poder para atentar contra derechos humanos e invadir la privacidad de las personas, sino también para evadir impuestos y protegerse de la regulación. Hemos pasado del mundo del internet libre y abierto al mundo de las grandes empresas no reguladas que controlan el dominio digital del que depende prácticamente todo. Es la privatización elevada a su máxima potencia.

Casi todos los aspectos de nuestra vida diaria que ahora suceden *online* están privatizados. Su infraestructura digital permea al Gobierno central y al local, a los servicios públicos, al transporte, las telecomunicaciones y la energía, a centros de trabajo, a las calles y a los hogares. La lista crece progresivamente a medida que todo

se digitaliza y, con ello, se vuelve más dependiente de las empresas que controlan las tecnologías y los sistemas que hacen posible esa digitalización.

Su alcance global les permite organizar sus identidades corporativas, ubicaciones y operaciones para eludir las leyes, restricciones y obligaciones fiscales existentes, algo que sus gobiernos les aseguran mediante acuerdos internacionales de libre comercio y normas *ad hoc* a menudo negociadas bajo el radar. Y, si las cosas no salen como quieren, sus gobiernos dan la cara por ellas. No hay más que ver cómo se puso a la defensiva el Gobierno estadounidense contra el impuesto de Francia del 3 por ciento sobre servicios digitales, más conocido como «tasa Google». Trump, entonces presidente, amenazó con imponer más aranceles a ciertos productos franceses. Al final la sangre no llegó al río, ya que la Oficina del Representante Comercial de Estados Unidos (USTR, por sus siglas en inglés) suspendió dicha medida, a la espera de que finalice su investigación sobre otros impuestos similares al francés puestos en marcha en otras diez jurisdicciones. Entre ellas se encuentra España, que, como la francesa, grava con un 3 por ciento los ingresos de las tecnológicas que facturen más de setecientos cincuenta millones de euros en total y más de tres millones de euros en España.

A pesar de algunas tímidas medidas legislativas como estas, los gobiernos siguen delegando la digitalización en los gigantes tecnológicos, que continúan atándoles las manos. La pandemia de coronavirus aceleró y exacerbó la tendencia, dado que era necesario facilitar la traslación de lo *offline* a lo *online* y hacerlo rápido.

A falta de tecnologías propias recurrieron a lo fácil: las de siempre. Los centros educativos son un ejemplo claro. Los recursos de trabajo en remoto, colaborativo y en tiempo real y las herramientas de videoconferencia y clases *online* de Google y Microsoft se instalaron en las escuelas sin cuestionamiento alguno ni búsqueda de alternativas competitivas. ¿Cuántos funcionarios implicados en esas decisiones comprendían realmente las implicaciones de lo que estaban negociando? ¿Cuál fue el escrutinio público del proceso?

Camino de privatizarse va también la justicia. Ya hace tiempo que en España y otros muchos países se ha reemplazado en gran medida a agentes humanos por cámaras de vigilancia y programas informáticos para detectar infracciones de tráfico y poner multas. También se usan programas de análisis masivo de datos para detectar el fraude fiscal, criticados por sus falsos positivos. Se planea asimismo ampliar su uso en el ámbito del trabajo, para multar a empresas por fraudes laborales. Todo ello sin un marco de referencia específico para el uso de estas tecnologías en la Administración Pública ni criterios de privacidad, transparencia o rendición de cuentas.

Más allá van países como Estonia, con el diseño de «robojueces», sistemas automatizados para resolver disputas asociadas a reclamaciones menores (de hasta siete mil euros). Por primera vez un algoritmo tomaría la decisión en primera instancia, aunque sus resoluciones podrían ser recurridas ante un tribunal humano. En

China, millones de casos se deciden ya en los llamados «tribunales de internet». Son procesos totalmente digitales en que los jueces son también sistemas automatizados basados en inteligencia artificial.

Con todo ello se busca supuestamente agilizar la justicia para que los jueces de carne y hueso puedan dedicarse a procesos de mayor relevancia; una idea que, en teoría, suena muy bien. El problema es que pasa por alto muchos obstáculos y riesgos asociados. Algunos son técnicos: los sistemas basados en algoritmos de inteligencia artificial avanzados tienen un funcionamiento opaco, por lo que no se puede saber cómo han tomado cada decisión.

Estos sistemas tampoco pueden contextualizar ni replicar las complejas consideraciones morales, las inferencias deductivas y el equilibrio de las razones en las que entra un juez humano, como explica la filósofa del derecho Lorena Jaume-Palasí. La ley es algo más que reglas y resultados deterministas; es una institución social sujeta a factores políticos, económicos y socioculturales que influyen en las concepciones prevalecientes de lo que es justo o injusto. Muchos conceptos jurídicos se construyen socialmente y no tienen significados singulares que puedan reducirse a un código binario de ceros y unos.

Usar algoritmos para la toma de decisiones judiciales iría, además, contra lo que Alain Supiot llama «la función antropológica de la ley»: proteger a los individuos y a la sociedad de los efectos potencialmente deshumanizadores de la ciencia y la tecnología. Al reemplazar a los jueces humanos por tecnología, esta se convierte en protectora y en aquello de lo cual debe protegernos. Pierde así su humanidad.

Todos estos procesos de digitalización —que no tendrían que ser negativos *per se* — se llevan a cabo desde una perspectiva tecnodeterminista que prioriza la computación como una forma superior y racional de toma de decisiones sobre la base de que los números no mienten. Es una visión limitada de la inteligencia humana que asume que las máquinas manejan mejor muchas áreas de la vida.

Yuval Noah Harari, el historiador y célebre autor de *Sapiens* y *Homo Deus*, le ha puesto nombre a esta tendencia que lo permea todo y a la que Supiot llamaba «gobernar por números»:[5] el «dataísmo». Lo describe como una religión que «sostiene que el universo consiste en flujos de datos, y que el valor de cualquier fenómeno o entidad está determinado por su contribución al procesamiento de datos». Se trata de un pensamiento ampliamente extendido por el que todo en el universo se explica por leyes matemáticas y se reduce a algoritmos, a corrientes de datos que pueden analizarse utilizando los mismos conceptos y herramientas básicos. Frente a los enormes y crecientes volúmenes de datos existentes y en proceso de generación, los dataístas consideran que escapa a los humanos la tarea de extraer de ellos información; una tarea que solo puede asumir, en su supuesta superioridad, la inteligencia artificial, la deidad del dataísmo.

Esta noción de que los conjuntos de datos masivos son repositorios que producen verdades fidedignas y objetivas ha sido también bautizada como «fundamentalismo

de datos». Este integrismo dataísta no considera factores complejos que influyen en qué datos se recopilan y cómo se manipulan para producir un resultado determinado. Como dice el catedrático de filosofía Daniel Innerarity: «La creencia de que la cuantificación produce la verdad privilegia una falsa idea de la objetividad y proporciona una certidumbre engañosa que impide un conocimiento cabal de la realidad».[6]

Los fundamentalistas de datos ignoran también que, si no se controlan, los algoritmos pueden codificar los sesgos y prejuicios sociales, acelerar la difusión de la desinformación y contribuir a robar la atención de los usuarios y convertirlos en adictos. A pesar de todo, caminamos hacia la consolidación de un sistema en el que lo que importa es lo cuantificable, los números; los datos que las tecnológicas, en el mundo del todo conectado, recogen y procesan. Es más, se delega en ellas (o directamente se usurpa) la toma de decisiones en cuestiones clave como el establecimiento de estándares técnicos para la infraestructura digital, para las carreteras y puentes de internet y de la vida digital.

El hecho de que esas carreteras, la infraestructura pública digital, nacieran en manos privadas conlleva a su vez riesgos críticos como el de no poder controlar la infraestructura de servicios esenciales en una crisis (pongamos una pandemia, un gran ciberataque o una caída de internet o de la electricidad). Eso por no hablar de la cantidad de datos sensibles que una infraestructura pública digitalizada genera y a los que tienen acceso las corporaciones privadas que la administran.

Todo esto refuerza las ataduras y dependencias con respecto a los gigantes tecnológicos, y también su poder. Al mismo tiempo, estos están sometidos a otros poderes igual de autoritarios o más: gobiernos represivos o amenazas criminales o terroristas, a cuyas presiones no siempre se resisten. Amnistía Internacional denuncia que plataformas como Facebook y YouTube se han convertido en terrenos de caza para los censores gubernamentales en Vietnam y también para sus troles contra el discurso crítico.[7] Les acusan de complicidad con la represión sistemática de contenido pacífico que se considera crítico con las autoridades mediante el bloqueo geográfico generalizado.

Ninguna de las dos empresas lo esconde. Facebook reconoce sin rubor sus restricciones de acceso a contenido que se opone al Partido Comunista y al Gobierno de Vietnam.[8] YouTube no desmiente lo obvio, alegando que cumple con las leyes locales de cada país.[9] El Gobierno vietnamita aseguró en octubre de 2020 que las tasas de cumplimiento de las solicitudes de censura de «mala información, propaganda contra el Partido y el Estado» por parte de Facebook y Google (propietaria de YouTube) habían alcanzado el 95 y el 90 por ciento, respectivamente,[10] su pico más alto hasta el momento.

Otras empresas como Netflix también ceden. La plataforma fue reprobada por bloquear un episodio de la comedia *Acto patriótico* a petición de Arabia Saudí. El motivo no fue otro que la crítica que en él se hace al príncipe heredero de la corona

del país árabe, Mohamed bin Salmán, algo que el Gobierno considera que viola sus leyes de delito cibernético. Netflix justificó la autocensura por su deber de cumplir con las leyes locales.

No es que las empresas de tecnología deseen someterse a los deseos y mandatos de los gobiernos. Estas ceden o no a sus presiones en función de lo que más pueda afectar de forma significativa a sus negocios. Censurar publicaciones está bien siempre que aún puedan publicitarse, pero los intentos de regularizar sus impuestos o poner límites a su modelo de negocio basado en la atención encuentran una fuerte resistencia.

RUPTURA SOCIAL

«Los tecnólogos son los planificadores urbanos del tejido social. Organizan los flujos de cableado de la atención humana, los términos y la base de las relaciones de las personas», dice el arrepentido extrabajador de Google Tristan Harris. Parece una exageración y probablemente lo sea, pero lo cierto es que Harris no anda tan descaminado.

La economía de la atención se basa en el conocimiento de la fragmentación social existente y ofrece antídotos para ese terreno hostil. Ofrece un cordón umbilical a través de un dispositivo que ancla la infraestructura digital al propio cuerpo, que, así, tiene la impresión de estar constantemente conectado al mundo.[11] Por tanto, se siente menos solo.

La soledad es una de las grandes epidemias de los tiempos modernos, como lo ha sido siempre. ¿Por qué ahora que tenemos a miles de personas al alcance de un clic, ahora que estamos conectados con mucha más gente, seguimos sintiéndonos tan solos? Somos seres sociales y como tales usamos estas herramientas: para socializar con otros, observar y ser observados. Esas recompensas que hacen que las redes sociales sean tan adictivas alimentan nuestro sentido de pertenencia, arraigada hace miles de años, cuando cada colectivo se repartía la búsqueda de alimento y la carga de trabajo para protegerse mutuamente ante los peligros del exterior.

Somos una especie social, y sentir que compartimos pedazos significativos de nuestras vidas con otras personas que nos reciben y abrazan es vital para nuestro crecimiento personal y nuestra salud psicológica e incluso física.[12] Sentirse integrado ayuda a superar en compañía fracasos amorosos y pérdidas, éxitos y contratiempos, en una comunidad íntima y especialmente solidaria.

Entonces ¿por qué hemos construido una sociedad individualista? ¿Por qué hemos creado un modelo que no tiene en cuenta que somos seres gregarios y que necesitamos al grupo? Hace apenas cien años vivíamos en núcleos de población mucho más pequeños, con una familia más extensa en una estructura social más colaborativa donde se desarrollaban vínculos duraderos y donde el propio grupo familiar y el vecindario actuaban como soporte.[13] Por el contrario, la vida ahora

tiende a desarrollarse en pequeños apartamentos en grandes ciudades donde se pierden los vínculos con el barrio, con unidades familiares cada vez más pequeñas. Nos sentimos más solos que nunca, aunque estemos rodeados de millones de personas, física y virtualmente.

Para paliar la soledad del modelo urbano y el aislamiento rural, acudimos a la tecnología que nos conecta con el mundo: internet. Primero fueron los chats (como el memorable IRC [Internet Relay Chat]) y ahora son las redes sociales. Las cifras hablan por sí solas. El porcentaje de adultos estadounidenses que utiliza las redes sociales aumentó del 5 por ciento en 2005 al 79 por ciento en 2019.[14] A escala global, Facebook pasó de cubrir alrededor del 1,5 por ciento de la población mundial en 2008 a alrededor del 30 por ciento en 2018.[15] Es un ejemplo extraordinario de cuán rápida y drásticamente pueden cambiar los comportamientos sociales: algo que hoy es parte de la vida cotidiana de un tercio de la población mundial era impensable hace menos de una generación.

Sin duda, esta puede ser una herramienta útil frente al sentimiento de marginación. Puede proporcionar cierto sentido de pertenencia a determinados individuos, interaccionando con gente que les escucha a miles de kilómetros. A primera vista puede parecer que las redes sociales ayudan a sentirse integrados, ya que proporcionan innumerables contactos. Sin embargo, estos medios se usan a menudo como un pretexto para evitar la comunicación significativa y las relaciones más profundas. Son relaciones menos comprometidas que no están destinadas a reemplazar amistades íntimas auténticas.

La sensación de soledad entre la multitud de la vida en grandes ciudades se replica en la red. Las redes sociales pueden ser un buen complemento del contacto humano, pero no un sustituto. Cuando se usan como tal (como reemplazo) se confunde la pertenencia con la popularidad medida en «Me gusta» o comentarios fugaces. Las redes sociales hipersocializan:[16] llenan nuestras pantallas con flujos constantes de actualizaciones de estado, noticias, historias, mensajes, tuits, comentarios, referencias, anuncios, notificaciones… Sin embargo, la recompensa inmediata de la hipersocialización, a la larga, solo genera vacío y malestar. No satisface la necesidad profunda de socialización y reafirma la sensación de soledad. De hecho, cuanto más tiempo pasan las personas en redes sociales, mayor es su insatisfacción y más solas se sienten.[17]

Las redes sociales crean un sustituto de la comunidad, pero, como sostenía el célebre sociólogo Zygmunt Bauman, no son una comunidad. Ello no evita que sean una mina de oro que explota el miedo de la mayoría de nosotros a ser abandonados, a quedarnos solos.[18] «La gente se siente un poco mejor porque la soledad es la gran amenaza en estos tiempos de individualización. Pero en las redes es tan fácil añadir amigos o borrarlos que no necesitas habilidades sociales. Estas las desarrollas cuando estás en la calle, o vas a tu centro de trabajo, y te encuentras con gente con la que

debes tener una interacción razonable. Ahí tienes que enfrentarte a las dificultades, involucrarte en un diálogo», dijo Bauman en una entrevista en 2016.[19]

Las redes son un producto de la «modernidad líquida» que el sociólogo definió hace más de veinte años, en los albores de internet. El mundo líquido nació con el cambio de era —del *hardware* al *software*— y en comunión con la globalización. Se caracteriza por un estado fluido, ligero, no estructurado, provisional, efímero y continuamente cambiante. Las relaciones sociales se enmarcan en la instantaneidad, el individualismo y el distanciamiento del otro. Los individuos se reducen a consumidores y la identidad se condiciona a los dictados de la sociedad de consumo. El nuevo modelo de socialización se basa en el individualismo y es, en realidad, un proceso de desocialización. Y este se ve agudizado por una nueva herramienta con un infinito potencial multiplicador: internet.

La red de redes se ha convertido en el nuevo gran elemento estructurador de la socialización, el gran catalizador del individualismo en red que caracteriza a las relaciones *online*. Internet proporciona una sensación de inclusividad que reemplaza el sentido de pertenencia por la suma social virtual. Una falsa sensación de agregación de elementos aislados —si acaso grupos— con vínculos frágiles. Una sociedad fragmentada que se desocializa y se desagrega.

En contraste con la vivencia de y en una sociedad física cercana que condicionaba nuestras decisiones egoístas, nos sumergimos en una sociedad *online* de miles de millones de internautas donde siempre hay algún grupo que se alinee con un gusto o una idea específico, por extravagante u oscuro que pueda ser. Una experiencia mediada por pantallas que, si bien da cabida a cualquier minoría, requiere de una menor capacidad de negociación y compromiso. Cuando no es necesario renunciar a la propia visión del mundo para sentirse parte del grupo, es fácil evitar el proceso de maduración y de autocuestionamiento.[20] Peor aún: los modos de hacer *online* se trasladan a lo *offline* y reconfiguran también en el mundo físico los procederes sociales y los modos de relacionarse. Condicionan y predefinen la interacción, eliminan la fricción, huyen del diálogo incómodo y cultivan relaciones efímeras o superficiales.

Asimismo se reconfigura la esfera pública, que es el espacio donde suceden el diálogo y la comunicación social; donde se expresa la participación ciudadana en una conversación abierta sobre las cuestiones de interés general y se desarrollan soluciones colectivas. Como es obvio por la naturaleza de internet y las redes sociales, esa plaza del pueblo se ha extendido a lo virtual. El escenario *online* brinda acceso a los excluidos, iguala (en teoría) las voces. Eso, en teoría.

En sus comienzos, las redes sociales fueron recibidas como ese espacio liberador y democratizador donde todas las corruptelas e injusticias quedarían expuestas, donde serían compartidas y condenadas prácticas execrables. Una poderosa herramienta de autoorganización para rebelarse contra los opresores. No se puede negar que en algo han contribuido a ello. A Twitter, Facebook y otras plataformas se debe parte del

éxito de la revolución democrática de la Primavera Árabe (2010-2012) que tumbó varios gobiernos. Los manifestantes usaron estas redes sociales para compartir información sin censura, para concienciar y autoorganizarse. También lo hicieron después movimientos como el español 15-M (2011), el estadounidense Occupy Wall Street (2011) o la Revolución de los Paraguas (2014), también conocida como Primavera Asiática.

Hoy la imagen que ofrecen esas plataformas es muy distinta. Han convertido el ideal de la democracia participativa en una máquina de hacer dinero. Sus algoritmos median la participación social y sus líderes tienen poder para decidir quién participa en la conversación, o a quién acallar. Es la comercialización y la privatización de la esfera pública *online*, un giro antidemocrático en el que son las corporaciones, y no las leyes, las que definen los límites del discurso permisible. Un descomunal ejercicio de poder aplicado a su antojo: se silencia a Trump y a algunos presidentes o jefes de Estado autoritarios pero a otros no, de forma arbitraria. Sin transparencia y sin rendición de cuentas.

La plaza pública deja de ser pública cuando el flujo de información y opiniones no es libre, sino mediado. Los algoritmos deciden qué mostrar y a quién, marcan las tendencias y lo que es más o menos visible. La igualdad de acceso a la plaza pública se difumina en la desigualdad de visibilidad, en la disparidad de eco que obtienen unas y otras voces.

Internet no es la causa de la fragmentación social, pero, como sucede en tantos otros aspectos, reproduce —o potencia— la realidad *offline*. La tecnología tiene potencial para desgarrar sistemáticamente el tejido social de la vida pública. Esta se centra en la abstracción, la generalización, la escala y el crecimiento. Sabe cómo universalizar, no cómo llegar a la raíz de las comunidades locales. Cuanto más se abstraiga y se generalice todo, más dividida estará la sociedad. Las guerras culturales *online* amplifican la fragmentación epistemológica (cómo sabemos lo que sabemos, o cómo accedemos al conocimiento), lo que a su vez fractura el tejido social. Es difícil construir una sociedad con personas que comparten diferentes entendimientos del mundo que les rodea.

La información puede ser un elemento de unión de comunidades. El problema con el acceso a esta a través de las redes sociales es que estas se fundamentan en que el conocimiento está dentro de los datos. Funcionan con el supuesto de que las personas harán clic para acceder a ese contenido, no simplemente a los titulares, como *de facto* sucede en la mayoría de los casos.[21] No solo no se lee el contenido, sino que se comparte sin haber sido leído. Ya en 2016 un estudio encontró que nunca se hace clic en el 59 por ciento de los enlaces compartidos en Twitter. En la misma línea van otros experimentos más informales o hallazgos casuales. Una periodista de *Upworthy* cuenta cómo un titular publicado por error en redes sociales sin enlace al artículo correspondiente fue compartido y obtuvo más de dos mil comentarios de personas que, por razones obvias, no habían podido hacer clic en él ni leerlo.[22]

A pesar de todo, el tejido social resiste. Pese a que pueda haber una inclinación *online* hacia la fragmentación y a aislarse en la burbuja propia y desconfiar más de los otros, el saldo neto de las relaciones *online* es a menudo positivo. Varios estudios[23] han encontrado que ciertos usos de la red de redes pueden aumentar el capital social. Este mide el alcance y la naturaleza de nuestras conexiones con los demás, el grado de cooperación y colaboración, confianza y compromiso cívico, las actitudes y comportamientos colectivos, cómo cada cual aprovecha para sí las oportunidades que surgen en estas relaciones.

Como las comunidades *online* no están vinculadas con los vecindarios, la gente moviliza capital social a través de una variedad de fuentes especializadas, en lugar de depender de un solo grupo muy unido de vecinos y parientes. Internet ayuda a los usuarios y usuarias a socializar virtualmente con nuevas personas, familiares y amigos. La contrapartida es que, al mismo tiempo, se tiende a disminuir la conexión con la comunidad local, el contacto en persona y las relaciones de proximidad (claramente no es el caso de Tinder ni de otras aplicaciones que conectan a las personas por cercanía geográfica). Menos comunicación cara a cara, menor participación en actividades sociales y familiares presenciales, y mayor desvinculación de los jóvenes en la participación comunitaria y aislamiento físico de los individuos.

Las relaciones sociales en los barrios se desmiembran progresivamente. Cada vez la gente conoce menos a sus vecinos y aumenta la tendencia a la segregación.[24] Las aplicaciones de recomendación que sugieren lugares que hay que visitar o dónde comer en función del nivel de renta también contribuyen a que no nos mezclemos. Es uno más de los múltiples ejemplos de algo cada vez más obvio: internet no es el escenario de una vida paralela, separada de la vida real. Lo *online* está entrelazado en los hilos del tejido social e integrado de forma indisoluble en el todo individual y social. La antigua realidad es suplantada por bases virtuales y ofrece una experiencia del mundo administrada por la tecnología.[25]

La infraestructura digital no es únicamente física o material, también es inmaterial, como bien apunta la especialista en filosofía del derecho Lorena Jaume-Palasí.[26] No solo los servidores y cables que hacen de carreteras y avenidas para circular *online*, sino cada algoritmo. Cada nuevo servicio *online* o aplicación añade un ladrillo más a toda la infraestructura inmaterial digital, una capa invisible de *software* que media las interacciones cibernéticas. Capas que constituyen los procesos *online* por defecto a base de secuencias computerizadas y a menudo automatizadas. Por ejemplo, cada red social establece el marco o interfaz en el cual se comparte contenido y estructura, condiciona y limita los formatos posibles y las formas de interacción.

Cuando usamos las aplicaciones estamos aceptando sus reglas. Cada una tiene unos valores, fines e instrucciones diferentes. Su estructura y el tipo de relaciones sociales que fomentan conducen hacia ciertos puntos de vista. La forma en que las

personas interactúan entre ellas y con el mundo que las rodea está determinada por los sistemas que utilizan, incluidas todas las aplicaciones y redes sociales. Estos sistemas constituyen la arquitectura de la comunicación, la dotan de normas y moderan las relaciones sociales. Se conforma así, de modo apenas perceptible y sin debate, una estructuración algorítmica de la sociedad y la conducta humana.[27]

Esa arquitectura responde a sus propios objetivos —los de las empresas que la crean—, que, salvo en contadas excepciones, son diferentes a los de quienes usan sus servicios. Si Google velase por la privacidad de los usuarios, tendría que renunciar a su modelo de anuncios hiperpersonalizados; si a Facebook le preocupase el bienestar de las personas, tendría que dinamitar su sistema de ingresos publicitarios basado en maximizar el tiempo que estas pasan en su plataforma. Ese bienestar de las partes implicadas no está entre los principales objetivos de estas compañías. Su fin es aumentar su valor en bolsa, y a eso responden su comportamiento y sus métricas. Es la meta para la cual están optimizados sus algoritmos.

La forma en la que crean infraestructura los sistemas digitales se basa en una personalización ficticia, solo a escala estadística, que permite la hipersegmentación de la publicidad. Esta individualización no se dirige a cada persona en concreto: no entiende de individuos, sino de medias y patrones. Proporciona a cada cual lo que una persona promedio con sus características necesitaría o desearía, lo cual puede diferir enormemente de lo que en realidad esa persona necesita o quiere. Esto explica muchas de las fricciones digitales. Además, y más grave aún, estructura la discriminación, al no tener en cuenta las diferencias individuales y basarse en promedios de mayorías, excluyendo a las minorías. Como es obvio, estos sistemas no están diseñados teniendo en cuenta una visión de impacto en lo colectivo ni en la cohesión social. Miran al bosque como a la suma granular de sus árboles en lugar de como un todo.[28]

LA CONTAMINADORA NUBE

> La humanidad se encuentra en una encrucijada con respecto al legado que deja a las generaciones futuras.
>
> DAVID COOPER, subsecretario ejecutivo del Convenio de Naciones Unidas sobre la Diversidad Biológica

A finales de 2020, la investigadora y directiva de Google Timnit Gebru fue despedida[29] por escribir y pretender publicar un artículo científico sobre los problemas éticos de los avances recientes en inteligencia artificial. En concreto, sobre el impacto ambiental y los sesgos de este tipo de tecnología. El texto ponía de manifiesto un estudio[30] sobre los costes medioambientales de entrenar un tipo de algoritmo avanzado de IA, que venían a ser de 284.000 kilogramos de dióxido de carbono. O, lo que es lo mismo, las emisiones equivalentes a cinco coches a lo largo de toda su vida útil, incluida la fabricación.

Son cifras de mínimos, dado que el desarrollo de estos modelos requiere no solo uno, sino varios procesos de entrenamiento. Estos sistemas resultan mejores cuantos más datos usan, y cuantos más datos usan, más energía consumen. Dado que internet es una fuente inagotable e *in crescendo* de este combustible algorítmico que se almacena en centros de datos con un elevado consumo energético, es de prever que las emisiones de CO_2 asociado sigan aumentando.

Solo considerando los centros de datos ya hablamos de alrededor de un 1 por ciento del consumo de la electricidad global, al que se suma otro 1 por ciento de las redes de transmisión de datos;[31] un total del 2 por ciento del consumo global. Si ampliamos a todo el espectro de las tecnologías de la información y las comunicaciones (TIC), la cifra asciende hasta el 7-11 por ciento[32] y se prevé que alcance el 21 por ciento —o hasta el 51 por ciento según los peores augurios— en 2030.[33]

El tráfico mundial de internet aumentó casi un 40 por ciento entre febrero y mediados de abril de 2020, durante el apogeo de la COVID-19.[34] Durante la última década —entre 2010 y 2020—, esta cifra se ha multiplicado por doce y el número de usuarios de internet en todo el mundo se ha duplicado: ya representa el 51 por ciento de la población mundial, y se prevé que ascienda al 66 por ciento en 2023.[35] Para ese mismo año, se espera que la cantidad de dispositivos conectados represente más del triple de la población mundial. Es decir, un crecimiento de casi un 40 por ciento en cinco años.[36]

Los datos no auguran buenas perspectivas. Se calcula que las TIC ya emiten un 4 por ciento de todo el CO2 global (cifra similar a las emisiones derivadas de la quema de combustible en la industria de la aviación), que podría duplicarse hacia 2025.[37] Hablar de estas tecnologías en abstracto puede dar una falsa sensación de distancia, pero las emisiones están asociadas a cosas tan mundanas como hacer búsquedas en internet, enviar *e-mails*, escuchar podcast o ver vídeos o contenido audiovisual en directo o bajo demanda. Esto último (la reproducción de vídeos) representa casi un 60 por ciento del tráfico de datos del mundo,[38] es decir, más de trescientos millones de toneladas.[39] Para hacerse una idea, esa cifra es mayor que las emisiones netas de CO_2 de toda España durante el año 2019.[40]

Otro proceso *online* controvertido por su consumo energético y emisiones es el asociado al medio de pago digital Bitcoin y a otras criptodivisas. La preocupación ambiental respecto al uso de Bitcoin surge de la gran huella de carbono que requiere el proceso de minado de blockchain, la tecnología subyacente a este sistema de transferencia de dinero digital. Estimaciones conservadoras sitúan el consumo eléctrico de esta actividad en más de 45 teravatios-hora (TWh) en 2018.[41] Traducido a CO_2 supuso entre 22 y 30 millones de toneladas de CO_2 ese año.

Las cifras en 2019 podrían haberse duplicado, según varios análisis.[42][43] Eso elevaría el gasto energético de esta criptomoneda a más de 87 TWh de energía

eléctrica anual, el equivalente a un país como Bélgica. En la actualidad ese consumo se cifra entre 77[44] y 121,36 TWh (más de lo que consume un país como Argentina).[45] Convertido a emisiones, hablamos —en el mejor de los casos— de una media anual de casi 37 millones de toneladas de CO_2.[46] Es decir, más que la huella de carbono de Nueva Zelanda.[47] Otras estimaciones sitúan el consumo anual de Bitcoin en casi un 0,7 por ciento del total de consumo energético mundial.[48] Y ello sin tener en cuenta el impacto medioambiental de otras criptomonedas. Bitcoin utiliza más de diez veces la cantidad de CO_2 que un billete tradicional.[49]

Considerando las cifras anteriores y el crecimiento acelerado de Bitcoin y de otras divisas digitales como Ether, estos métodos de pago podrían igualar el total global de transacciones sin efectivo en menos de cien años.[50] Eso asumiendo que siguiera la tendencia de crecimiento medio observada en la adopción de otras tecnologías. Puede ir incluso a más, a juzgar por el auge de las *non-fungible token* (NFT), o TNF (token no fungible) una especie de certificado digital de autenticidad y propiedad de una obra de arte que solo existe en formato electrónico y que está validado por tecnología blockchain o similar.

De seguir así, las emisiones acumuladas resultantes podrían calentar el planeta unos 2 °C entre once y veintidós años, según el ritmo de adopción.[51] Eso siempre y cuando los tipos de combustibles utilizados para generar electricidad (el *mix* energético) se mantuvieran en los valores actuales.

Las compras *online*, como toda actividad en internet, se traducen también en emisiones. Durante el pico del confinamiento por la COVID-19 en 2020 casi diecinueve millones de personas adquirieron productos por vía telemática, lo que supone un 7 por ciento más que el año anterior.[52] Un 51 por ciento de esas personas aumentó la frecuencia de las compras *online*, una tendencia que llega para quedarse.[53]

La cuestión es: ¿genera más CO_2 comprar en tiendas físicas o hacerlo en internet? Un estudio realizado en el Reino Unido concluyó que esta última opción genera casi el doble de emisiones (de gases con efecto invernadero) que en el caso del comercio tradicional, pero solo cuando la web donde se compra no tiene un establecimiento asociado.[54] Al contrario, la compra *online* mixta (en sitios web o *apps* de tiendas físicas que prestan servicio de entrega a domicilio) es la forma más eficiente en términos de energía. Esta opción tiene también, de media, menor impacto medioambiental que el comercio tradicional, aunque depende de las prácticas y elecciones de los consumidores en cada lugar (si van a comprar en su coche o si, por el contrario, lo hacen caminando, en bicicleta o en transporte público).

Otro gran problema medioambiental es el de la basura eléctrica y electrónica derivada, entre otros, de los teléfonos inteligentes, tabletas, ordenadores y dispositivos conectados. El consumo creciente de productos tecnológicos ha aumentado exponencialmente la generación de esta clase de desecho que contiene componentes muy contaminantes. Es el tipo de residuo de más rápido crecimiento en

el mundo:[55] un total de más de cincuenta y tres millones de toneladas en 2019, a razón de más de siete kilogramos por persona. Es el mayor volumen registrado hasta la fecha.

A escala mundial, Asia es el mayor generador de basura electrónica, de la que menos de un 12 por ciento se recolecta y se recicla adecuadamente.[56] En España se generaron, en 2019, 888.000 toneladas de residuos de este tipo, que se traducen en una cifra individual muy superior a la media: 19 kilogramos por persona. ¡19 kilos por cabeza! Un enorme saco de patatas lleno de chatarra electrónica que cargamos a nuestras espaldas cada doce meses. Es el efecto del comprar-tirar-comprar, de la fiebre de las tendencias y «lo nuevo», y de la obsolescencia programada que muchas empresas de tecnología profesan. Entre ellas Apple, que ya ha sido condenada en Italia[57] o Estados Unidos[58] por limitar la vida útil de algunos dispositivos. En España, la Organización de Consumidores y Usuarios (OCU) también ha demandado por estos motivos a la empresa de la manzana.

Entre cifras y cifras llegan las dosis de realidad: multiplicación de incendios que llegan hasta Silicon Valley, deshielo acelerado, nevadas nunca vistas, olas de calor en niveles máximos, desaparición de especies, catástrofes (anti)naturales… Un colapso catastrófico de la biodiversidad biológica —que disminuye a un ritmo sin precedentes — y una degradación de ecosistemas que amenaza con acabar con la inestimable diversidad genética y que pone en peligro el suministro de alimentos, la salud, la seguridad y la propia supervivencia humanas.[59]

Solo la contaminación del aire por la quema de combustibles fósiles es ya responsable de una de cada cinco muertes en el mundo.[60] Es un total de nueve millones de personas. Representan uno de cada diez fallecimientos en Europa y Estados Unidos, y casi un tercio de las muertes en el este de Asia. Eso sin contar otras derivadas mortales del cambio climático. Y, como dice el subsecretario ejecutivo del Convenio de Naciones Unidas sobre la Diversidad Biológica, David Cooper, «las cosas solo empeorarán si no cambiamos de rumbo».[61]

¿Y SI…?

Las cosas solo empeorarán si no cambiamos de rumbo. La frase de Cooper es igualmente aplicable a la deriva de internet. No será muy difícil imaginar qué nos deparará el futuro de seguir las cosas así: más de lo mismo, más consolidado y, en muchos casos, peor y más extremo. Es la única cuasi certeza entre el desasosiego, cuando las seguridades de antaño se han desvanecido. Son, como diría de forma jocosa Douglas Adams en su *Guía del autoestopista galáctico*, las áreas rígidamente definidas de duda y de incertidumbre.

Quedarnos sin internet podría ser un drama. Para algunos, imaginarlo es un alivio. Pero no es lo mismo desconectar de forma voluntaria que un apagón de internet por un ataque intencionado, como no es igual decidir quedarse en casa una semana, o un

«finde», que un confinamiento forzoso en el contexto de una pandemia. ¿Y si decidiéramos, colectivamente, dar un paso atrás y deshacernos de la red de redes? Liberación para unos, tragedia para otros; fracaso, para todos, del mayor invento —probablemente— desde la electricidad. El recuerdo de lo que pudo haber sido y no fue. La vuelta a la caverna, tal vez. O el momento del reencuentro.

Sin embargo, el fracaso se puede evitar. El futuro no está escrito, lo que significa que aún se puede escribir. No hay necesidad de tomar decisiones drásticas como acabar con internet. Lo que es seguro es que habrá que hacer elecciones difíciles a todos los niveles. Preguntarse, primero, ¿y si las cosas no tienen por qué ser así? Hay un tema común en las discusiones sobre tecnología que la trata como una fuerza externa, de alguna manera imparable e inevitable, que los humanos somos incapaces de cambiar. Nos han convencido de una visión del progreso tecnológico y de la innovación como bienes sociales inalienables que deben incentivarse a toda costa. Ello sirve como pretexto para imponer más control y vigilancia sobre los procederes humanos; para promover, blanquear y objetivizar las políticas neoliberales tradicionales más dañinas y mantener el *statu quo*; para seguir privatizando la gobernanza y el poder. Si ello implica cargarse la cohesión social o el planeta, es lo de menos.

Esa visión trata de hacer ver que el ciudadano de a pie, ustedes y yo, somos meros espectadores sin nada que decir al respecto. Las obvias asimetrías de poder contribuyen a la mirada del individuo corriente y moliente como una pequeña persona *versus* la enorme máquina de hacer dinero. Sus impulsores conforman el «patriciado tecnológico» que retrata José María Lassalle,[62] un poder sin relato y sin necesidad de legitimarse. Un poder que no se han ganado en las urnas: se lo hemos dado, sin más, los consumidores y usuarios. «Sucumbimos ante un poder sobrenatural, inevitable, que nos ciega bajo la embriaguez digital», dice Lassalle.

Prueba esa embriaguez la carta de Larry Page. «¿Qué podría ser mejor?», se preguntaba este de forma retórica. Es la asunción ciega de que cualquiera estaría de acuerdo en que nada podría ser mejor que el monopolio totalitario que él y sus colegas de Silicon Valley esperan que continúe dominando el mundo, determinando la estructura de internet y nuestro futuro colectivo. Su ideal de progreso inevitable tiñe de negro el futuro en un mundo que parece haber desistido de aspirar a un porvenir mejor; un mañana en el que nos convertimos en objetos inertes, y no en sujetos de nuestras vidas.

La sensación de inevitabilidad es, como dice Shoshana Zuboff, un «narcótico existencial».[63] Conlleva la inacción y la parálisis. A ella responden y contribuyen los imaginarios que construyen las ficciones distópicas, tan presentes en todas las formas de entretenimiento. Esta época dorada de la ficción distópica está impregnada de una nueva literatura y ficción televisiva de pesimismo radical que enferma las quejas y complace resentimientos.[64] Una «ficción de la sumisión» frente a la «ficción de la resistencia» que practicaban George Orwell o Aldous Huxley.

En las distopías modernas, la llamada a la resistencia se ha ido por el sumidero. Su única advertencia es una mayor desesperación. Alimentan el pesimismo conservador y la cultura de la queja, refuerzan los lamentos y acomodan a la inacción. Carecen de ánimo y de fuerza propositiva. Fomentan el temor, el miedo paralizante, sin proponer alternativas. No imaginan un futuro mejor ni le piden a nadie que se moleste en hacerlo.

El foco central de las distopías modernas es la tecnología, la gran culpable. Surgen como reacción a un sistema que no vincula la emancipación con hacernos más sabios, sino más ricos; que nos ha hecho creer que prosperidad y progreso es igual a riqueza; que nos ha convertido en una pieza más en el engranaje del frenético avance tecnológico sin control.

La tecnología es la cabeza de turco. Pero la tecnología es inerte, no tiene intención. No es neutra, pero su falta de neutralidad no es voluntaria ni propia, sino inducida y ajena: le es insertada por quienes la desarrollan, que a su vez siguen los mandatos de quienes la diseñan, que a su vez responden a quienes la conciben u ordenan concebirlas y pagan y ponen los medios para ello. Insertan en su estructura un modo de ver el mundo y unos valores. Lo hacen en el marco de un sistema que permite e incentiva desarrollos tecnológicos de usos perversos, que los acepta sin ser consciente de ello, ni de cómo esos «avances» impactan en la sociedad.

Internet, la gran plataforma de conocimiento, una de las mayores creaciones de la humanidad, se ha convertido en un nido de dependencia, adicción, vigilancia, desinformación, manipulación y censura que amenaza con su propia destrucción. Lo que se creó como una manera de conectar al mundo para colaborar ha terminado en una forma más de control y de optimización del *statu quo* que profundiza en nuestras divisiones, miedos y brechas; pero internet, *per se*, no es el problema. Tampoco lo son el big data y la inteligencia artificial, ni las redes sociales.

El problema es en qué se basan estas infraestructuras, qué reglas tienen o de cuáles carecen, cómo funcionan, a qué objetivos responden, cómo y para qué se usan, qué castigan y qué premian. La prueba está en todo lo bueno para lo que también pueden usarse y, *de facto*, se usan estas herramientas. Toda esa tecnología y esas plataformas a las que se presupone ser fuente de todos los males presentes y futuros llevan décadas mejorando la vida de las personas. ¿Vamos a renunciar a ello? No, no hay por qué. No, las cosas no tienen por qué seguir como hasta ahora. Y sí: hay esperanza ante el abismo.

El sentimiento de incapacidad para cambiar el curso del imparable «avance» tecnológico es razonable, pero cuando miramos hacia atrás y vemos por qué internet se ha desarrollado como lo ha hecho vemos que es el resultado de decisiones tomadas por los humanos. Por tanto, es razonable también creer que los humanos pueden —podemos— tomar decisiones para cambiar el camino futuro de internet. Como dijo Henry Ford: «Tanto si crees que puedes hacerlo como si crees que no, tienes razón».

La revista británica *The Economist* publica anualmente un especial titulado «The world if».[65] Es un ejercicio de imaginación de futuros posibles más o menos inmediatos o de presentes alternativos que podrían ser reales de haberse dado condiciones diferentes en el pasado: «El mundo en 2022 si la COVID-19 hubiera devastado la aviación», «El mundo a partir de 2050 si la industria de eliminación de carbono reemplaza a la industria petrolera», «El mundo hoy si la energía nuclear hubiera despegado en la década de 1970»…

De igual modo podemos plantearnos: ¿y si perdemos definitivamente la batalla de la gobernanza? ¿Y si llevamos al extremo la ruptura social? ¿Y si dejamos que colapse por completo el medio ambiente? O, por el contrario, pensar: ¿y si todo hubiera sido un mal sueño? ¿Y si despertamos del letargo para construir un nuevo internet descentralizado, abierto, libre de monopolios, cooperativo, donde la tecnología de datos y la inteligencia artificial son usadas para el bien, con un tejido social reconstruido y un nuevo contrato social?

¿Y si volvemos a confiar en que un mundo mejor es posible? En realidad, lo es, y hay muchos ejemplos reales de ello. Los conoceremos en el siguiente capítulo.

10

Volver a confiar

Usa la Fuerza, Luke.

OBI-WAN KENOBI,
La guerra de las galaxias, episodio IV: *Una nueva esperanza*

Nadie en Wall Street lo vio venir. ¿Qué impacto podrían tener un puñado de chiquillos jugando a desestabilizar el mercado financiero? En la era preinternet, posiblemente nulo. Hoy, en la red, todo es posible. En enero de 2021 un grupo de aficionados a la bolsa logró aumentar más de un 1.700 por ciento el valor de las acciones de la cadena de tiendas GameStop, que habían tocado suelo nueve meses antes. La hazaña —que dio la vuelta al mundo— les hizo ganar unos cuantos millones y causó pérdidas multimillonarias a los fondos especulativos imperantes en la Bolsa de Nueva York.

Los autores de la «proeza» eran ni más ni menos que un ejército de inversores minoristas profanos, en su mayoría jóvenes veinteañeros que vivieron la crisis de 2008 como adolescentes. Su punto de encuentro era —y es— un foro del portal *online* Reddit llamado *wallstreetbets* (algo así como «apuestaswallstreet»). Su *modus operandi* es la guerra de guerrillas. A través de la plataforma, se ponen de acuerdo para hacer subir los precios (a corto plazo) de aquello que les interese y así obtener dinero rápido.

Los «guerrilleros» de *wallstreetbets* aprovechan los puntos débiles del sistema para manipular los precios. Llevan años haciéndolo, aunque nunca con una acción tan duradera y con tal impacto. La revolución de GameStop fue tal que solo fue posible aplacarla prohibiendo o limitando la compra de acciones de la compañía, forzando así el *game over* de los inversores. El patrón se replicó con otras empresas como Blackberry o Nokia y el movimiento llegó hasta España, donde miles de pequeños inversores se juntaron en Telegram para montar un *wallstreetbets* a lo español.

El suceso hizo que el antiintervencionista Wall Street se tambaleara hasta el punto de que las autoridades financieras estadounidenses tuvieron que plantearse tomar medidas para mantener la integridad de los mercados. Al mismo tiempo, puso de manifiesto cómo el sistema financiero beneficia a los grandes jugadores en lugar de a los inversores individuales. Es la historia de David contra Goliat, de la fuerza de internet y su poder para multiplicar el impacto de la acción colectiva. O, lo que es lo mismo, la historia del poder de las comunidades *online*, de personas corrientes y molientes que pueden organizarse para ponerlo todo al derecho, o del revés.

El propósito de *wallstreetbets* puede no gustar, pero su caso sirve como ejemplo de lo que se puede gestar en la red de redes y de su potencial huella, para mal o para bien. Otros ejemplos conocidos son la Primavera Árabe, el 15-M, Occupy Wall Street, la Revolución de los Paraguas, el #MeToo, o #DeleteUber y #DeleteFacebook. ¿Recuerdan #DeleteFacebook? El movimiento «borra Facebook» surgió en redes sociales a raíz del escándalo de Cambridge Analytica en 2018, cuando se conoció que la red social había recopilado datos de millones de usuarios de la aplicación sin su consentimiento y se los había facilitado a Cambridge Analytica, que los usó para ayudar a la campaña presidencial de Trump en 2016.

La presión pública llevó a Mark Zuckerberg a testificar ante el Congreso estadounidense por el uso indebido de datos de los usuarios. El movimiento concienció a gobiernos y usuarios de la importancia de la privacidad y de que es necesario regular la recopilación y uso de datos personales masivos por parte de las empresas tecnológicas. Facebook no se quedó sin usuarios, pero sí perdió a buena parte de ellos. En Estados Unidos, un 42 por ciento se tomó un descanso de la aplicación, mientras que un 25 por ciento la borró por completo.[1] Entre los que se quedaron, la mitad hizo un ajuste en su configuración de privacidad.

Las acciones de Facebook se desplomaron (cayeron más de un 24 por ciento en una semana).[2] Dos meses después la Unión Europea aprobó el Reglamento General de Protección de Datos (RGPD). Un año después, la Comisión Federal de Comercio de Estados Unidos (FTC) multó a la empresa con cinco mil millones de dólares.[3] Se iniciaron cambios legislativos y nuevas regulaciones que cristalizaron en la Ley de Privacidad del Consumidor de California,[4] que otorga a los consumidores californianos más control sobre la información personal que las empresas recopilan sobre ellos. Todo ello obligó a algunas compañías a revisar toda su infraestructura de datos. Algunas, como Twitter, Slack o Instagram, ya habían hecho algunas modificaciones en 2018, también a raíz del movimiento #DeleteFacebook.

Esta no es la única campaña contra la red social o el poder de las tecnológicas. Ha habido más después de #DeleteFacebook y también antes. El antecedente más directo es #DeleteUber, movimiento nacido en Twitter como castigo a una acción de la compañía que causó indignación entre los usuarios. Fue en enero de 2017, cuando Donald Trump anunció una orden ejecutiva que prohibía a refugiados e inmigrantes de ciertos países entrar en Estados Unidos. En respuesta a la prohibición hubo diversas protestas, y entre ellas una huelga de taxistas en el aeropuerto de Nueva York. En ese momento, Uber no solo continuó ofreciendo su servicio de transporte privado en el aeropuerto, sino que anunció en Twitter que había desactivado su función de aumento de precios en momentos de alta demanda. El gesto fue visto como una acción oportunista de la compañía y un usuario de Twitter inició la campaña #DeleteUber. Como resultado, más de doscientas mil personas eliminaron la aplicación de su móvil.[5] Incluso el director general de Uber se vio obligado, tras las

críticas, a abandonar el Consejo Asesor de Asuntos Económicos de Trump, al que pertenecía.

TODOS A UNA

La comunidad científica también se organiza *online*. La pandemia de la COVID-19 lo puso claramente de relieve como la gran villana. El día en que China anunció su primera muerte oficial por la infección, el biólogo Eddie Holmes publicó la secuencia genética del virus en un sitio web llamado virological.org.[6] Ese simple acto, la posibilidad de compartir el ADN del SARS-CoV-2, fue crucial para los investigadores de todo el mundo. La «zona cero para la lucha científica contra la enfermedad», como lo llama el propio Holmes. Fue el comienzo de un esfuerzo global sin precedentes. Algo que, en condiciones normales, habría llevado diez años de trabajo se veía condensado en meses. Un hito que la conectividad hizo posible.

A los científicos se unieron otras muchas comunidades en todo el mundo. Eclosionó un movimiento global para paliar la escasez de equipos de protección personal y de respiradores, necesarios para asistir a las personas afectadas que requerían ventilación mecánica. Los hospitales no estaban preparados para cubrir una demanda tan alta, y acelerar su producción no era fácil. Dado que se trata de dispositivos de soporte vital, tienen que ser absolutamente fiables, pero producir sistemas así requiere muchas pruebas que pueden prolongarse hasta dos años. Los pacientes que ya estaban llenando las unidades de cuidados intensivos no disponían de ese tiempo.

De forma instintiva, el movimiento *maker* (de «Hazlo tú mismo», *Do It Yourself*, o DIY) y la comunidad de *software* libre se pusieron en marcha. Personas de todo el mundo activaron sus redes *online* para diseñar respiradores de forma conjunta, fabricarlos y probarlos, y ponerlos a disposición de los centros sanitarios. En paralelo, centros de investigación e instituciones como la NASA se volcaron también con este propósito. Los gobiernos y las autoridades sanitarias pidieron la colaboración de industrias y universidades para la fabricación de ventiladores, como así fue. Hasta los equipos de Fórmula 1 se implicaron en ello.

En España nacieron múltiples iniciativas, como el Foro CoronavirusMakers, y, dentro de él, subgrupos, como Reesistencia o Freesterra, además de otras, como The Open Ventilator o Aire-19. Estas se dedicaron al diseño y desarrollo de ventiladores replicables de bajo coste, y varias de ellas fueron homologadas por las autoridades sanitarias. Las soluciones resultantes no solo salvaron vidas en España, sino que llegaron a varios países de Latinoamérica. Paralelamente se formaron otros movimientos con distintos proyectos como COVIDWarriors, nacido para tratar de canalizar la voluntad de los integrantes de la comunidad *online* IP (Interesting People) de ayudar en la lucha contra la enfermedad.

En cuestión de semanas, los COVIDWarriors lograron diseñar, comprar y traer a España unos robots con los que multiplicar la velocidad de obtención de resultados de las pruebas PCR, que especialmente al comienzo de la pandemia suponían un cuello de botella en la contención del virus. Movieron cielo y tierra para importar, reconstruir, acondicionar y montar las cuatro primeras instalaciones (cuarenta y cuatro robots en cuatro grandes hospitales), a las que les siguieron catorce hospitales más, en catorce provincias. Un total de ciento noventa y ocho robots capaces de hacer un millón de PCR al mes. No contentos con esto, crearon un robot autónomo —ASSUM— capaz de erradicar cualquier bacteria y virus como el SARS-CoV-2 en pocos minutos, destinado a esterilizar instalaciones hospitalarias, o lo que hiciera falta. Todo esto lo lograron, internet mediante, con la ayuda de cientos de voluntarios, filántropos y mecenas, colaboradores privados que facilitaron la logística de forma altruista, empresas y centros hospitalarios.

Es solo uno de los muchos hitos de este grupo que ya ha recibido varios premios. Tiene abiertos, además, multitud de proyectos centrados en ayudar tanto a profesionales sanitarios como a pacientes y a la población en general. Iniciativas para mejorar la ventilación de espacios, para reducir la brecha digital, para levantar el ánimo o para afrontar la despedida de seres queridos. IP, la comunidad *online* en la que nació este movimiento de «guerreros» contra la COVID-19, fue creada por el pionero del internet español Andreu Veà en 2008 para juntar a todo tipo de personas interesantes, inquietas o «mentes brillantes» dispuestas a ayudar a los demás sin esperar nada a cambio. Hoy son (o somos, dado que yo misma formo parte de ella) casi dos mil personas en noventa y ocho ciudades de los cinco continentes que han puesto en marcha múltiples iniciativas y proyectos.

Todas estas iniciativas son meros ejemplos entre una vastísima cantidad de movimientos *online* autoorganizados en torno a la lucha contra la pandemia. El universo de comunidades *online* es realmente eso, un enorme universo. Algunas son generalistas y otras más especializadas o hiperespecializadas. Como en el caso de los proyectos anticoronavirus, en ellas surgen multitud de proyectos y subproyectos que son una fuente de generación de conocimiento y de soluciones digitales (o incluso materiales) que pasan al acervo común digital. Por ejemplo, los ventiladores desarrollados en código abierto, material de protección para profesionales sanitarios y para el público en general, y otros desarrollos.

Estas soluciones han sido creadas de forma colectiva, y cualquier persona en cualquier parte del mundo conectada a internet puede replicarlas o mejorar su diseño. De igual modo sucede con otros millones de creaciones abiertas y accesibles *online*, desde herramientas informáticas o materiales de cualquier tipo y para cualquier cosa (incluido el manejo de la salud) hasta recursos informativos. No hay límite más allá de las necesidades y voluntades humanas de creación e invención, y de la imaginación.

Ese acervo común *online*, el «procomún digital», son los bienes comunales digitales que se crean o se mantienen en internet y tienen forma de conocimiento, datos, código, tecnología, información, cultura, etc. Son compartidos, accesibles a todo el mundo y abiertos a que cualquiera construya sobre ellos. La Wikipedia es el ejemplo por antonomasia: una enciclopedia libre, colaborativa, multilingüe y gratuita, creada y mantenida por una comunidad de editores voluntarios. Nació en 2001 y es una de las webs más visitadas de todo internet, con más de cincuenta y cinco millones de artículos.[7]

Antes de la Wikipedia se creó la gran biblioteca de la red, Internet Archive. Es otra iniciativa legendaria. Comenzó en 1996 archivando el contenido que se generaba en internet y hoy dispone ya de más de veinte años de historial web al que cualquiera puede acceder. También empezó a digitalizar libros, imágenes, vídeos y hasta programas de televisión. Hoy almacena cuatrocientos setenta y cinco mil millones de páginas web y decenas de millones de libros, textos, audios, vídeos e imágenes, además de casi seiscientos mil programas de *software*.[8]

Internet Archive y la Wikipedia son parte y símbolo del inmenso tesoro del procomún digital que se ha alimentado y fraguado gracias a movimientos surgidos en los primeros años de internet, antes incluso de que Berners-Lee creara la web. El origen de esos movimientos estuvo vinculado con el campo del desarrollo de programas informáticos: el movimiento del *software* libre fundado por el controvertido[9] programador Richard Stallman para contrarrestar el auge de programas informáticos de propiedad privada.

Stallman pensaba que cualquiera debería tener libertad para ejecutar este tipo de sistema para cualquier propósito, cambiarlo a su antojo y distribuir copias y los cambios realizados. Gran parte de la red troncal de la internet actual se basa en ello. La filosofía que hay detrás de lo que se convertiría en un movimiento masivo otorga libertad a los usuarios. Según Stallman:

> Con el *software* libre, los usuarios tienen el control del programa, tanto individualmente como de forma colectiva. Así controlan lo que hace el ordenador […].
> Con el *software* propietario, el programa controla a los usuarios, y alguna otra entidad (el desarrollador o «propietario») controla el programa. De modo que el programa privado da al desarrollador poder sobre los usuarios. Eso en sí mismo es injusto.[10]

Las palabras del programador siguen vigentes y explican gran parte de los problemas actuales con la tecnología. De ahí que se acuda al *software* libre y de código abierto como paradigma alternativo con potencial para mejorar la vida, al abrir el acceso a los recursos y crear nuevas áreas de autogestión colectiva y gobernanza. También de generación de riqueza: el valor del código abierto solo en la Unión Europea asciende a sesenta y tres mil millones de euros al año, o el 0,4 por ciento del PIB.[11] Cada

empleado a tiempo completo que desarrolla código abierto genera cuatro veces más PIB.

Esas potencialidades se han visto reforzadas por otras herramientas, como las licencias Creative Commons, que permiten a los creadores compartir sus obras con cualquier usuario, sin que este tenga que solicitarle permiso al autor de la obra, y hacer que patentes y derechos de autor estén disponibles gratuitamente. Hoy, todo ello se ve aumentado por las nuevas posibilidades de la tecnología conectada, la internet de las cosas, la inteligencia artificial o los sistemas de fabricación digital e impresión 3D. La innovación tecnológica democratiza los medios de producción y facilita que se aproveche el potencial creativo. Internet permitió eliminar intermediarios para ponernos en contacto globalmente de manera virtual, una frontera que ahora pasa a lo físico para conectarnos también a recursos y herramientas.

Las comunidades de bienes comunales creadas entre pares a través de la red son la esencia de lo que se pretendía crear con internet: un espacio libre, abierto y colaborativo. Estos espacios se pueden usar para crear conocimiento, recursos y bienes para todo tipo de fines. A ello responde la eclosión de la cultura *maker* y el DIY. A través del acceso compartido a herramientas y tecnologías de fabricación digital antes restringidas al ámbito corporativo, cualquiera puede convertirse en fabricante. Esto contribuye a democratizar la invención y la innovación. Se multiplican las posibilidades de creación y, por tanto, el rango del procomún digital. Ello se traduce, además, en la posibilidad de crear productos realmente personalizados, hechos a la medida de quien los produce o de colectivos altamente segmentados que no encuentran en el mercado soluciones para sus necesidades hiperespecializadas (a menudo poco rentables para las empresas).

Así se crean comunidades por nichos. Por ejemplo, personas con paraplejía que se conectan entre ellas y diseñan sillas de ruedas adaptadas a su cuerpo o sus rangos de autonomía; o padres de hijos con diabetes que antes no tenían acceso a dispositivos muy caros para controlar los niveles de glucosa de sus pequeños y, a través de estas comunidades, han podido crearlos o acceder a ellos.[12] Algunas personas incluso consiguen descifrar el código de dispositivos privados para mejorarlos. Es el caso del español Víctor Bautista, cofundador de la aplicación SocialDiabetes, que abrió los entresijos del medidor de glucosa Freestyle Libre para poder integrarlo con su *app*. Además, esos datos se pueden compartir para investigar conjuntamente aspectos que afectan a perfiles tan específicos que no se consideran altamente relevantes para la ciencia.[13]

Las creaciones del movimiento de código abierto y *maker* a menudo se financian también de forma colectiva, entre pares. Lo hacen, de nuevo, a través de plataformas *online*, donde pueden acceder a inversores, mecenas o donantes de todo el mundo. Es lo que se conoce como *crowdfunding*, con importes de microfinanciación que pueden ir desde unos escasos euros hasta unos cuantos miles. Puede darse de diversas

formas: como donativo, a cambio de una recompensa, a modo de inversión o como préstamo.

Las plataformas de *crowdfunding* desintermedian el acceso a la financiación y lo descentralizan, sin necesidad de entidades financieras de por medio. Permiten incluir a los usuarios o posibles clientes en el proceso, saber qué funciona mejor o peor, interactuar con ellos… Todo tipo de proyectos de código abierto se financian por esta vía: aplicaciones de audio, para el hogar o el automóvil, dispositivos de salud, etcétera.

A veces, estos proyectos acaban convirtiéndose en empresas. Entre la multitud de ejemplos está el popular Makey Makey, un kit de invención que permite a niños y adultos convertir objetos cotidianos en controladores táctiles conectados a internet. Nació como proyecto académico de dos estudiantes del laboratorio Media Lab del Instituto Tecnológico de Massachusetts (MIT) y ahora es un negocio con una comunidad de miles de colaboradores. El éxito de su campaña de *crowdfunding* lo hizo posible: recaudaron una cifra veintidós veces mayor que la que esperaban (casi quinientos setenta mil dólares).

Otros proyectos nacen con ánimo de lucro desde el comienzo (que sean de código abierto no significa que sean gratis). Uno que triunfa es el dispositivo asistente de voz Mycroft Mark, que promete hacer sombra a Google Home y Alexa sin tener que renunciar a la privacidad. En su segunda versión, Mycroft Mark II, consiguió recaudar veinte veces más de lo que se proponía entre dos plataformas de *crowdfunding* (casi un millón de dólares en total).

PODER CIUDADANO

Tras el desastre nuclear de Fukushima, un grupo de ciudadanos desarrollaron y financiaron colectivamente el dispositivo SafeCast para recopilar y compartir datos abiertos sobre los niveles de radiación ambiental en su territorio.[14] Ante las insuficientes o poco fiables mediciones de radiación oficiales publicadas por el Gobierno, decidieron actuar. No habrían podido hacerlo, o no en tan poco tiempo y de forma tan innovadora, de no ser por los recursos de código abierto y los datos abiertos existentes, las herramientas de fabricación digital y el talento de personas de todo el mundo.

En este contexto surgieron numerosos proyectos que buscaban ayudar a manejar la situación y proporcionar soluciones para mejorar su gestión. Es lo mismo que ocurrió durante la pandemia de la COVID-19 con grupos de científicos, *makers* y ciudadanos de a pie. Ninguna de esas iniciativas habría sido posible en tiempo y forma sin internet. Gracias a la red de redes y a su combinación con otras nuevas tecnologías han proliferado los movimientos y comunidades que se valen de herramientas tecnológicas y digitales para contribuir a la vida cívica. Es lo que se conoce como «tecnología cívica» o *civic tech*.

Las tecnologías cívicas buscan desbloquear las barreras institucionales y abrir espacios de participación ciudadana.[15] Se trata de que los ciudadanos participen en el funcionamiento de las ciudades y en las decisiones que afectan a sus barrios, más allá de votar cada cuatro años. Las iniciativas en torno a la *civic tech* pueden dirigirse a mejorar las funciones estatales, las capacidades organizativas de las instituciones públicas y los procesos de toma de decisiones públicas; a aumentar la calidad de vida (servicios de salud, educación, accesibilidad, etcétera); a abordar los desafíos complejos de las sociedades (discriminación, brecha de género…); a apoyar el medio ambiente mediante la creación de herramientas de transporte y consumo sostenibles o de reducción de desperdicios, o a fomentar la transparencia y rendición de cuentas por medio de estrategias de datos abiertos, accesibles y comprensibles.[16]

En las tecnologías cívicas lo importante, en realidad, no es la tecnología, aunque esta sea un elemento característico. Una *civic tech* puede ser simplemente una web. Como tal nació Change.org, una plataforma de peticiones ciudadanas en la que cualquier persona o grupo de la sociedad civil puede realizar su denuncia o reivindicación y recoger firmas de apoyo. Las campañas con mayor impacto llegan a cambiar políticas públicas o incluso a salvar vidas. Le sucedió a la adolescente sudanesa Noura Hussein, que había sido condenada a muerte por apuñalar a su violador, con el que había sido obligada a casarse cuando era una niña. Más de 1,7 millones de personas firmaron la petición para evitar que la condenasen a morir.[17] La petición se entregó en las embajadas sudanesas de seis países y recibió el respaldo del secretario general de la ONU. Debido a la presión, los funcionarios sudaneses acordaron revocar la sentencia de muerte y reemplazarla por una pena menor.

Change.org es hoy una plataforma ampliamente conocida, que en su día daría el pistoletazo de salida a otras similares. Este tipo de iniciativas tienen sus orígenes en la «informática comunitaria», que desde los años setenta explora formas de aprovechar la tecnología para fomentar el capital social y empoderar a las comunidades locales.[18] Uno de los casos más conocidos es el de Blacksburg Electronic Village, una iniciativa de la Virginia Polytechnic Institute and State University (VPISU), en asociación con la ciudad estadounidense de Blacksburg y la compañía telefónica local. En 1991, se propusieron ofrecer acceso a internet a todos los ciudadanos de la ciudad, para apoyar y mejorar con ello la vida y las actividades cotidianas de sus habitantes. Como resultado, la ciudad se convirtió en la primera del mundo en adoptar un modelo totalmente *online* para una red comunitaria y fue pionera también en tener conectividad en hogares, escuelas y negocios. Proyectos como este han permitido la formación de comunidades digitales y han fomentado el capital social, han dado voz a colectivos a menudo marginados, han apoyado el desarrollo de la alfabetización tecnológica entre los ciudadanos y han desarrollado infraestructuras para permitir la acción ciudadana en asuntos de interés.[19]

Internet y los dispositivos conectados se unen a otras tecnologías, como los sensores, usados como herramientas para las iniciativas comunitarias ciudadanas. Por

ejemplo, para medir y monitorear colectivamente parámetros relacionados con el medio ambiente. Es lo que hicieron los vecinos del barrio de Gràcia (Barcelona) en 2017, hartos de los ruidos de las multitudes concentradas en la plaça del Sol hasta altas horas de la madrugada. Ello llevó a un grupo de residentes, en colaboración con el Fablab Barcelona y la investigadora Mara Balestrini, a investigar y hacerse con sensores para medir los niveles de contaminación acústica que había alrededor de la plaza.[20] Las mediciones, que llegaban directamente a una aplicación móvil, permitieron demostrar que el volumen de ruido llegaba a duplicar los niveles permitidos. Con el conocimiento en la mano y la identificación de posibles soluciones en común, el Ayuntamiento de Barcelona pudo definir unas políticas públicas basadas en las recomendaciones colectivas de los vecinos: renovaron la plaza e instalaron jardineras decorativas y un parque infantil para potenciar otro tipo de usos del espacio.

Como esta, muchas iniciativas de tecnología cívica nacen en comunidades locales. Otras parten de investigadores que detectan problemáticas y posibles vías de solución, y se dirigen a los vecinos para abordarlas de manera conjunta. Algunas surgen como emprendimientos sociales o en forma de organizaciones sin ánimo de lucro y otras como respuesta de los gobiernos y las administraciones públicas a un clamor popular.

Iniciativas, sean éstas más o menos informales, hay miles.[21] Su efectividad varía. Las intervenciones puntuales han demostrado una alta eficiencia y capacidad para lograr los objetivos propuestos. También para fomentar la innovación en la colaboración social y para nutrir el capital social.[22] Más complicado es lograr la integración de herramientas de tecnología cívica en la vida diaria de los ciudadanos, como sí lo han hecho otras muchas aplicaciones. Además, su alcance es sesgado y corre el riesgo de dejar fuera a personas con menor alfabetización digital y tecnológica.

La tecnología cívica se suma a las *govtech* en su propósito de cerrar la brecha entre unas instituciones estancadas en los modos de hacer del pasado, que no reflejan la sociedad de su tiempo, y una realidad que ha cambiado radicalmente y los ha dejado desfasados; en definitiva, contribuir a modernizar la democracia. Las *govtech* son tecnologías aplicadas a servicios públicos y de gobierno. Pueden dirigirse a mejorar las interacciones entre ciudadanos y administraciones públicas, a impulsar la participación ciudadana o a facilitar o cambiar la forma en que el Estado ofrece servicios, haciéndolos más eficientes. Ello implica normalmente —aunque no solo, ni siempre— la digitalización de los servicios públicos.

COMPARTIR ES VIVIR

La historia de la humanidad es una historia de compartir y no de poseer. Desde el Paleolítico, los cazadores-recolectores colaboraban y lo compartían todo.[23] Un

modo de vida que imperó durante millones de años hasta la llegada de la agricultura, con el almacenamiento privado de la cosecha. Se empezó a extender entonces el concepto de «propiedad privada» y, más tarde, el de «trueque» o «intercambio de bienes». Las primeras monedas eran productos básicos y útiles en sí mismos, como la sal, las especias o el ganado.

A escala individual y social, la filosofía de compartir, intercambiar y colaborar ha estado siempre presente. Ello ha tenido su correspondiente traslación a lo *online*: desde música, juegos, vídeos, artículos, contenido, ideas, investigaciones o desarrollos informáticos hasta artículos y productos físicos, y más recientemente acceso a otros bienes y servicios, como alojamiento o transporte.

En la sala de estar del informático Pierre Omidyar en California (Estados Unidos) nació en 1995 el primer gran referente de este modelo. AuctionWeb era un portal digital de subastas que permitía transacciones directas entre personas. Hoy se la conoce como eBay y es un negocio multimillonario presente en mil quinientas ciudades, con más de ciento ochenta y cinco millones de compradores y diecinueve millones de vendedores.

Poco después de eBay apareció Napster, la primera gran plataforma de intercambio de música en internet, con transacciones también entre pares. Paralelamente surgieron otras plataformas para el intercambio *online* de archivos de todo tipo, sin ánimo de lucro. Y, en la década de 2000, Zipcar popularizó el negocio de los automóviles compartidos de uso por horas o días: el *carsharing*.

El gran momento de la economía colaborativa llegaría, no obstante, una década después. En 2011, la revista *Time* eligió la economía colaborativa como una de las diez grandes ideas que cambiarían el mundo. Lo hizo en pleno auge de Airbnb, que fue uno de sus máximos exponentes. Airbnb nació de forma natural como la extensión digital del tradicional *bed and breakfast*, un servicio de cama y desayuno ofrecido por particulares. Pronto se convirtió en la sensación del momento y creció hasta lo que es hoy: una plataforma con cuatro millones de anfitriones presente en casi todos los países y regiones del mundo. Puso patas arriba la industria hotelera y se convirtió en un gigante que, en diciembre de 2020, salió a bolsa.

Airbnb hizo visible el modelo colaborativo. Vinculado con su éxito y con el de otras plataformas, como la francesa BlaBlaCar (para compartir trayecto en coche), está el florecimiento de otras muchas iniciativas con el modelo de alquiler o intercambio entre pares. Algunas ya existían y se hicieron populares, otras tantas vieron la luz en las dos primeras décadas del siglo XXI. Las hay para todo: compartir casa o intercambiarla, compartir vehículo y/o viaje, compartir espacio de trabajo, *parking* o habilidades; de trueque o segunda mano, de donaciones o inversión entre pares (el *crowdfunding*), etc.

Estos intercambios —salvo los relacionados con el alojamiento— ocurren principalmente a escala local o de vecindario. Para facilitarlos se han creado multiplataformas como Nextdoor, que es a la vez una red social para conectar con

vecinos, organizarse y compartir información y un espacio donde intercambiar, prestar o donar bienes y servicios, hacer recados o poner anuncios.

Asociados al modelo colaborativo están los modelos bajo demanda, de acceso y la economía *gig* (todos bajo el paraguas de la «economía de plataformas»). En la economía bajo demanda existe entre los usuarios una relación comercial y se da a cambio de una contraprestación[24] (por ejemplo, Glovo, Clintu o TaskRabbit). La economía de acceso se basa en una empresa que pone a disposición unos bienes para su uso temporal, como pueden ser vehículos de todo tipo (Car2go, Ubeeqo) o espacios de trabajo compartido o *coworking*.[25] La economía *gig* ofrece trabajo temporal con personas que ejercen como contratistas independientes[26] y en ella entran también Glovo o TaskRabbit, además de Cabify o Uber.

Como hemos visto, muchas de estas plataformas son controvertidas, especialmente por lo que a precarización del trabajo se refiere. También se ha acusado a algunas de ellas de adoptar los valores del movimiento colaborativo, basado en la comunidad, para perseguir sus propios intereses económicos. Su errónea y a veces malintencionada o interesada asociación con el modelo colaborativo le ha valido mala fama al segundo, pero no son lo mismo. Denominada inicialmente «consumo colaborativo»,[27] uno de sus pioneros en España —Albert Cañigueral— define la economía colaborativa como la manera tradicional de compartir, intercambiar, prestar, alquilar y regalar redefinida a través de la tecnología moderna y las comunidades. Se basa en sistemas de intercambio organizado, trueque, préstamo, comercio, alquiler, obsequio e intercambio. La intermediación entre la oferta y la demanda se genera en relaciones entre particulares, empresas o de particular a profesional, a través de plataformas digitales que no poseen los bienes que se van a compartir o intercambiar ni prestan los servicios asociados.[28]

Este modelo brinda a las personas los beneficios de la propiedad con una carga y un coste personal reducidos y también un menor impacto ambiental. Debido a esta naturaleza, la economía colaborativa genera un aprovechamiento eficiente y sostenible de los bienes y recursos ya existentes e infrautilizados y permite utilizar, compartir, intercambiar o invertir los recursos o bienes, exista o no una contraprestación entre los usuarios.[29] Su crecimiento y pervivencia la han consolidado hoy como una alternativa a las formas tradicionales de compra y propiedad.

Las plataformas colaborativas, en la medida en que posibilitan interacciones novedosas entre las personas, la comunidad y su entorno, son también tecnologías cívicas. En torno a ellas surgen iniciativas y proyectos de ciudades que buscan fomentar nuevas formas de propiedad colectiva de los bienes y servicios urbanos. Son las ciudades colaborativas, que aspiran a ser más que ciudades inteligentes. El ideal de ciudad colaborativa se centra en conectar las dimensiones tecnológica, económica y humana, y también en reconocer nuevos actores en el modelo de gobernanza urbana

e impulsar su colaboración. El papel del Gobierno local es servir como habilitador para identificar, nutrir y desarrollar el capital social de la ciudad.

En ese camino avanzan pioneras como Seúl (Corea del Sur). En 2012, su alcalde decidió apostar por este modelo ante los límites de crecimiento, en el sentido tradicional, de la ciudad. El propósito: aumentar el aprovechamiento de recursos y reducir el desperdicio, crear nuevas oportunidades económicas y fortalecer las relaciones de confianza. Otras ven este modelo también como una forma de proveer de servicios que el Gobierno no puede cubrir, no solo en las ciudades, sino también en zonas rurales.

Algunas ciudades colaborativas están centradas en la utilidad pública y otras en la inclusión o en el emprendimiento. Uno de los ejemplos más visibles de iniciativas de ciudades colaborativas se enmarca en la movilidad compartida, con flotas de vehículos (bicicletas, coches, motos) de uso público que muchos ayuntamientos de todo el mundo han puesto en marcha y que pueden reservarse mediante una aplicación móvil. Otro ejemplo son los presupuestos participativos,[30] que permiten a los habitantes decidir a qué se destina una parte de los fondos de la ciudad a través de plataformas *online*.

Setenta ciudades de todo el mundo, integradas en la red Sharing Cities Action, han declarado su intención de convertirse en colaborativas. Entre ellas varias españolas: Barcelona, A Coruña, Madrid, Santiago de Compostela, València y Vitoria. Entre sus líneas de acción están: impulsar la innovación pública, promover políticas que estimulen las plataformas con un impacto positivo sobre la ciudad, o defender y adaptar los derechos laborales y los derechos digitales.

EL SUEÑO DE LOS OBJETIVOS DE DESARROLLO SOSTENIBLE (ODS)

En 2030 habremos puesto fin a la pobreza y al hambre, cualquiera tendrá acceso a salud y educación de calidad, se habrá cerrado la brecha de género, habrá agua para todos, los países serán menos desiguales, la producción y el consumo serán sostenibles, habremos vencido al cambio climático y salvado los océanos, bosques y animales, reinarán la paz y la justicia y viviremos en armonía y aliados. Es el sueño de los Objetivos de Desarrollo Sostenible (ODS) para la Agenda 2030 adoptada por la ONU.

Estamos a menos de diez años del límite fijado para alcanzarlos y la tecnología claramente puede contribuir a acelerar la llegada a la meta. O, más bien, a las ciento sesenta y nueve metas en las que se subdividen los diecisiete ODS. Internet y las Tecnologías de la Información y la Comunicación (TIC) son parte del problema (que puede dificultar la consecución de los objetivos) y, a la vez, parte de la solución. Las TIC pueden lograr resultados a una escala, velocidad, calidad, precisión y coste que no se podían imaginar hace apenas una década.

La banda ancha móvil es una infraestructura esencial para los ODS. Multiplica la accesibilidad, escalabilidad y asequibilidad necesarias para cerrar numerosas brechas de desarrollo de forma rápida.[31] Junto con la internet de las cosas (IoT), la robótica avanzada, la fabricación digital e impresión 3D y la inteligencia artificial, puede acelerar las mejoras en acceso a salud, educación, energía y protección del medio ambiente. Puede reforzar la infraestructura y ayudar a afrontar la exclusión social y económica.

Las TIC son un catalizador para los tres pilares del desarrollo sostenible: desarrollo económico, inclusión social y protección del medio ambiente. Son una herramienta para alcanzar todos los ODS. Para el ODS 1 —fin de la pobreza— se ha demostrado cómo las TIC pueden aliviarla al promover el desarrollo social y la participación de las personas en la economía.[32] Por ejemplo, en zonas rurales de la India se ha logrado la práctica reducción de la pobreza mediante el desarrollo de proyectos TIC para mejorar las oportunidades de personas con pocos recursos de participar en la economía y acceder a los mercados y centros de salud y educativos.

Para el ODS 2 —hambre cero— las TIC pueden aumentar la eficiencia, la productividad y la sostenibilidad de la agricultura mediante información y conocimientos.[33] Por ejemplo, con redes de sensores conectados inalámbricos para el control remoto de sistemas de riego que, además, ahorran energía. El agua limpia y el saneamiento (ODS 6) pueden facilitarse con sistemas de gestión inteligente del agua mediante TIC.

En el ODS 3 —salud y bienestar— los ejemplos son múltiples. La era del todo conectado y las tecnologías móviles, en combinación con la pandemia de la COVID-19, han acelerado el desarrollo y la adopción de la telemedicina, las terapias digitales y el abordamiento personalizado, que permiten la asistencia sanitaria remota en cualquier rincón del mundo. La contribución de internet y las tecnologías móviles al acceso a la educación —ODS 4— también se ha precipitado con la pandemia. Tener un dispositivo conectado abre las puertas a la educación a distancia, a clases *online* y a oportunidades educativas de calidad. Pero, claro, para eso hace falta cerrar la brecha digital de acceso a una internet de calidad.

La igualdad de género (ODS 5), o más bien la brecha de género, está relacionada con la exclusión histórica de las mujeres de los campos de tecnología intensiva.[34] Si bien está claro hoy que no hay motivos para continuar perpetuándolo, sigue habiendo una gran ausencia de mujeres en ciencia y tecnología, especialmente en puestos de liderazgo. La brecha salarial de género se suma a las anteriores. Las TIC pueden igualar el acceso a la formación y las oportunidades, pero también están perpetuando los sesgos históricos a través de algoritmos viciados.

Hablando de desigualdades, el ODS 10 se propone reducirlas, pero de momento las TIC están dando una de cal y otra de arena. Internet y las tecnologías móviles tienen el potencial de ayudar a reducir la desigualdad en tanto que puerta de acceso a información, conocimiento y oportunidades para los colectivos más necesitados y los

países en desarrollo, pero eso no sucederá sin cerrar la brecha digital. Tampoco ayuda el enriquecimiento monopolístico de las grandes empresas tecnológicas, que contribuye a lucrar al 1 por ciento más rico.

En cuanto a las oportunidades de trabajo decente y crecimiento económico (ODS 8), es indiscutible la contribución de las TIC a este último. Más discutible es la derivada del trabajo decente, ya que han traído tanto prosperidad para unos como precariedad para otros. Nada que, por otra parte, no se pueda solucionar. En industria, innovación e infraestructura (ODS 9), las TIC llevan décadas promoviendo la convergencia total y fijando su foco en transformar las industrias convencionales y estimular la innovación.[35] Ahora ponen asimismo las miras en desarrollar una industrialización e innovación sostenibles.

Sostenibles también se quieren hacer las ciudades y comunidades (ODS 11). Aquí entran las ciudades inteligentes y colaborativas que aprovechan recursos y gestionan de manera eficiente la energía. Para serlo, se valen de las tecnologías cívicas y de gobierno, de internet, tecnologías móviles, herramientas de fabricación digital, sensores, IoT, big data e inteligencia artificial o blockchain. No hay que olvidar, sin embargo, la huella de carbono de estas tecnologías. Para que su aportación a la consecución de una producción y consumo responsables (ODS 12) sea positiva, es necesario alimentarlas de energías limpias y reducir la basura electrónica.

El acceso a una energía asequible y no contaminante (ODS 7) enlaza con la capacidad de las tecnologías conectadas de desarrollar y promover procesos energéticamente eficientes. Ello también contribuye a la acción por el clima (ODS 13), la cual se vale de las TIC para la obtención de mediciones más precisas de la huella de carbono, para la vigilancia y monitoreo de la meteorología y el clima, y para actuar en la prevención de desastres. Asimismo, pueden ayudar a la supervisión de los océanos y la preservación de la vida submarina (ODS 14) y de los ecosistemas terrestres (ODS 15), tanto en el seguimiento mediante satélites y sensores como en los análisis de grandes volúmenes de datos que indiquen tendencias y permitan hacer predicciones.

A la paz, la justicia y las instituciones sólidas (ODS 16) contribuyen las tecnologías que facilitan la gestión de crisis y la ayuda humanitaria, por una parte, y el gobierno abierto, la administración electrónica y la transparencia, por otra. Como se necesitan alianzas para lograr todos estos objetivos (ODS 17), las TIC facilitan la interconexión global.

Actualmente hay miles de proyectos encaminados al uso de internet y las TIC para acelerar la consecución de los ODS. Muchos de ellos ya han tenido un impacto positivo. El resto está por ver.

ALGO ESTÁ CAMBIANDO

Tecnología para el bien, o *tech4good*. Todo lo anterior podría entrar dentro de ese paraguas, en el que internet ejerce como elemento facilitador. Pero todo lo anterior es solo una parte del todo global. La etiqueta y las iniciativas *tech4good* nacen como distintivo de aquellos desarrollos y proyectos destinados a tener un impacto positivo en la humanidad, a poner las herramientas tecnológicas al servicio del bien común. Surgen como respuesta a una realidad hastiada de promesas rotas —de tecnología que no busca el bien común—, donde el *tech4good* no es la norma, sino una reacción contra esta; donde internet ha pasado de constituir un gran invento para mejorar nuestras vidas y la sociedad a ser la aparente (solo aparente) causa de todos nuestros males.

En la época de la Revolución Industrial a esa reacción se la llamó «ludismo». Ahora hablamos de *techlash*. A diferencia de antaño, el *techlash* no es una reacción contra la máquina —o contra el algoritmo— ni propugna, por lo general, la destrucción tecnológica. Más que rechazar las herramientas o desear su desaparición, apunta al inmenso poder y monopolio de las grandes corporaciones tecnológicas, y a su impacto social negativo.

Internet se ha convertido en una fuente de conflicto interno. Seguimos viendo colas para comprar el último iPhone, las redes sociales continúan atrayendo a millones de usuarios y Google no ha perdido el monopolio de las búsquedas, aunque estas acciones están cada vez más asociadas a un sentimiento de culpabilidad y rechazo. El *techlash* emana de ese rechazo y se vale, de hecho, de la tecnología para neutralizar sus efectos negativos.

La reacción creativa del *techlash* ha llevado al surgimiento de todo tipo de aplicaciones, filtros y estrategias para preservar la privacidad de los usuarios y su mapa de conexiones personales, herramientas contra ciberataques, utilidades para saber cuánto tiempo dedicamos cada día al móvil y a qué aplicaciones en específico, iniciativas de verificación y sistemas automatizados para detectar noticias falsas y discriminación, instrumentos de rastreo de las emisiones personales de CO_2 por el uso de sistemas informáticos, redes sociales alternativas sin manipulación ni recopilación salvaje de datos, estrategias contra correos no deseados y un largo etcétera.

Las GAFAM (Google, Amazon, Facebook, Apple y Microsoft) no son ajenas a ello y tratan de mostrar su lado amable con herramientas contra la desinformación (mientras sus algoritmos la premian), iniciativas educativas (mientras implantan sus sistemas propietarios y de vigilancia en centros de enseñanza), ayudas a medios de comunicación (mientras se niegan a pagarles por indexar su contenido), programas de sostenibilidad (mientras generan toneladas de CO_2), iniciativas para dar a la gente más control sobre sus datos (al tiempo que por otro lado se lo quitan)… El problema es claro: las acciones positivas no compensan. Tan solo representan una millonésima parte de su negocio. La ecuación entre unidades de acción perjudicial y unidades de acción apropiada sale en números rojos.

Algo parecido pasa en internet. La ecuación hace tiempo que empezó a salir en números rojos. Afortunadamente, algo está cambiando. El *techlash*, la *tech4good* y la internet de pares y del procomún demuestran que otra internet es posible si las cuatro «C» de la Fuerza de la red —conectar, colaborar, compartir y cocrear— nos acompañan. Con ellas se acerca el principio del fin. En el siguiente capítulo exploramos caminos posibles para un nuevo comienzo.

11

El principio del fin

Todo fin de la historia también contiene un nuevo comienzo; este comienzo es la promesa, el único «mensaje» que el final puede producir. Comenzar, antes de que se convierta en un hecho histórico, es la capacidad suprema del hombre; políticamente, es idéntico a la libertad del hombre.

HANNAH ARENDT, *Los orígenes del totalitarismo*

Debemos recuperar lo que hemos perdido: el derecho a conocer y a decidir quién sabe sobre nosotros, a decidir sobre nuestro futuro. Tales derechos han sido y siguen siendo las únicas bases posibles para la libertad humana y una sociedad democrática funcional.

SHOSHANA ZUBOFF[1]

Hablas como si Dios hubiera hecho a la Máquina, pero la ha hecho el hombre. No olvides eso.

E. M. FORSTER,
La Máquina se para

Dado lo mucho que ha cambiado la web en los últimos treinta años, sería derrotista y poco imaginativo suponer que la web, tal y como la conocemos, no se puede cambiar para mejor en los próximos treinta años. Si renunciamos a construir una mejor web ahora, entonces la web no nos habrá fallado. Nosotros habremos fallado a la web.

TIM BERNERS-LEE[2]

¿Y si Wikipedia estuviera en manos privadas, fuera de pago y con ánimo de lucro, y estuviera plagada de anuncios? Entonces, ya no sería Wikipedia. Tendría tal vez ese nombre, pero no su esencia, una esencia que habría estado muy cerca de perder de no ser por la rebelión española. Corría 2002 y, por aquel entonces (un año después del nacimiento de la enciclopedia), había muy pocos editores de la edición española de la Wikipedia. Cuatro personas fueron suficientes para frenar el intento de incluir en ella publicidad y hacer negocio con las aportaciones de contenido.

Edgar Enyedy, Juan Antonio Ruiz Rivas, Gonis y Javier de la Cueva pensaron que, si se llevaban a otra parte la Wikipedia en español, los gestores de la Wikipedia global verían las orejas al lobo. Efectivamente, así fue: los «cuatro fantásticos» trasladaron la edición española a un servidor externo y, al ver que desaparecía un idioma con tantos usuarios, los capos de la Wikipedia decidieron dar marcha atrás.

Así es como la «enciclopedia libre» de internet se convirtió en un procomún digital. [3] Su gestión pasó de una empresa privada (Boomis Inc.) a la Wikimedia Foundation, una organización estadounidense sin ánimo de lucro cuya fuente principal de financiación son las donaciones.

Wikipedia es hoy un símbolo de la internet utópica: un espacio abierto, colaborativo y libre, sin fines lucrativos, donde se comparte contenido con ánimo de aportar al conocimiento y sobre la base de información objetiva. «Hoy es imposible pensar en internet sin pensar en Wikipedia. Demuestra, ante todo, que un modelo basado en la colaboración altruista es posible», dice De la Cueva. En efecto, otra internet es posible. Otro modelo de negocio digital es posible e imprescindible. Pero el cambio hay que empujarlo, no va a suceder solo.

El *techlash* es un claro síntoma del hartazgo ciudadano. En España, crece sustancialmente la percepción de los efectos indeseados y las facetas negativas en la utilización de las tecnologías digitales, que asciende a un ocho sobre diez.[4] Preocupan en especial los riesgos en aspectos como la protección de la privacidad, la veracidad de la información, el acoso o el exceso de publicidad. El 67 por ciento de los usuarios de internet utiliza las redes sociales; sin embargo, la mayoría resalta más las facetas negativas que las positivas y cree que la información que en ellas se difunde es, por lo general, falsa.

Las consecuencias de este *techlash* que se extiende en el mundo digital se empiezan a notar. A finales de 2019, coincidiendo con el comienzo de la campaña electoral por la presidencia de Estados Unidos, Twitter anunció la prohibición permanente de anuncios políticos en su plataforma para tratar de evitar la manipulación del debate político en la red social. Un año después, ya en pleno proceso electoral, Google y Facebook imitaron la medida de forma eventual, a pesar de que en un principio se habían negado a hacerlo.

Las aplicaciones de mensajería también sufren los efectos del *techlash*. Ya a comienzos de 2021 WhatsApp comenzó a advertir a sus usuarios de la transferencia obligatoria de datos entre la *app* de mensajería instantánea y Facebook. La respuesta fue inmediata: millones de usuarios huyeron en desbandada. En solo setenta y dos horas, veinticinco millones de personas migraron a Telegram. Signal, otra aplicación de chat más respetuosa con la privacidad, pasó de tener poco más de un millón de usuarios hace un año a casi treinta millones a finales de enero. Aunque la nueva política de privacidad de WhatsApp no afectaba a la Unión Europea (ya que el Reglamento General de Protección de Datos [RGPD] no lo permite), la fuga de usuarios también se dio en Europa. Para muchos fue la excusa perfecta para plantearse usar alternativas menos invasivas con la intimidad.

Como abanderada de la privacidad de los usuarios quiere mostrarse Apple, que ha estado limitando la cantidad de datos que las aplicaciones pueden recopilar sobre los usuarios y obligando a los proveedores a ser más transparentes al respecto. Ya permite, incluso, rechazar por completo la recopilación de datos en la que se basa el

negocio de muchas de esas *apps*. La medida le valió una disputa pública con Facebook, que se la tomó como un ataque directo contra la compañía (la reina del rastreo y uso de datos personales de los usuarios).

Que Apple facilite herramientas para bloquear el rastreo de información íntima está muy bien, pero es un parche que no resuelve el problema de base. Esas continuas invasiones de la privacidad no se deberían dar en primer lugar, y no tendríamos que necesitar soluciones para limitarlas o impedirlas. ¿Qué mundo es este en el que la gente tiene que andar escondiéndose por las esquinas? Lo que hace falta no son tecnologías de camuflaje, sino libertad para ser sin necesidad de ocultarse.

Eso es lo que se nos niega: la libertad de vivir y desarrollarnos en entornos indeterminados y no predeterminados por la tecnología, de ser soberanos de nuestra propia vida y de estar *offline*. Esa es la amenaza del determinismo tecnológico para la humanidad; el canto de sirena de los sistemas supuestamente inteligentes que prometen una felicidad barata; un mundo de felicidad óptima que ignora el asesinato del futuro humano.[5]

Dice Zuboff que hay que reavivar la sensación de indignación y pérdida ante lo que se nos ha quitado; rechazar la inevitabilidad; negarnos a ceder el futuro al poder ilegítimo; romper el hechizo de fascinación, impotencia y resignación; fijar el rumbo; reclamar que el capitalismo funcione como fuerza inclusiva vinculada con el pueblo al que debe servir.[6] Es la fuerza que debe empujar el cambio. O, mejor dicho, los múltiples cambios. No hay varitas mágicas, ni soluciones rápidas ni fáciles, ni botón que apretar para pasar de un estado a otro. Se requieren medidas a muchos niveles, escalas y contextos, a menudo interdependientes. ¿Por dónde empezamos?

ALIANZA DEMOCRÁTICA POR LA GOBERNANZA DIGITAL

Hacia el final de la Segunda Guerra Mundial, los aliados reconocieron que necesitaban establecer nuevas instituciones para apoyar la prosperidad y la paz. En julio de 1944 representantes de cuarenta y cuatro países se reunieron en Bretton Woods (New Hampshire, Estados Unidos) para definir el nuevo orden financiero mundial. El acuerdo facilitó la creación de estructuras clave en el mundo financiero: el Fondo Monetario Internacional (FMI) y el Banco Mundial (BM).

A escala política, se creó la Organización de las Naciones Unidas (ONU), centrada en mantener la paz, desarrollar relaciones amistosas entre naciones y fomentar la cooperación y el respeto a los derechos humanos. De cincuenta y un países iniciales se ha pasado a ciento noventa y tres estados miembros.

La creación de estas instituciones se enfrentó a un entorno geopolítico que cambió muy pronto, cuando descendió el Telón de Acero y congeló al mundo en los dos bandos opuestos de la Guerra Fría. Las instituciones recién creadas también se bifurcaron: la URSS no refrendó el acuerdo de Bretton Woods y la misión de la ONU

de mantener la paz colapsó en un mundo de lucha de las dos superpotencias del momento: Estados Unidos y la URSS.

Hoy nos encontramos en un periodo similar de crisis, oportunidades y cambio geopolítico. La pandemia no solo demostró cuán dependientes somos de internet, sino cómo las cosas pueden cambiar rápidamente cuando hay voluntad política. Si antes se aceptaba que no podíamos tener lo bueno de internet sin lo malo, existe una creciente demanda de que eso cambie. Hay quienes creen que esto requiere de una solución global, pero lamentablemente eso es cada vez menos posible. China hace tiempo que inició la separación de la red de redes global, y ahora Rusia lo está haciendo también, ambas para servir a sus propias necesidades antidemocráticas.

Esta división es importante porque «arreglar» internet no solo implica ponerse de acuerdo en aspectos comerciales, sino de derechos humanos y de los trabajadores, de seguridad y muchos otros. Basta con mirar la frecuente ineficacia de la ONU para saber que las democracias y las autocracias no están lo suficientemente de acuerdo como para actuar (esperemos que el cambio climático, como amenaza existencial para el planeta, sea una excepción). De igual modo, tratar de solucionar a escala global los problemas de gobernanza de lo digital a los que nos enfrentamos no conducirá más que a cumbres y documentos que quedarán enterrados en un cajón, cuando lo que se necesita son acciones colectivas.

Una alternativa que sí podría funcionar es crear un frente común de las democracias, donde los valores compartidos sean los suficientes y lo suficientemente fuertes como para que sea posible un cambio real. A esto lo llamo la «Alianza Democrática por la Gobernanza Digital». Y hago una llamada explícita a la historia: uno de los desafíos fundacionales de la Sociedad de Naciones en 1919, después de la Primera Guerra Mundial, fue que Estados Unidos no se uniera. Esta vez, Estados Unidos y la Unión Europea deben ser los promotores de este esfuerzo.

Ese frente democrático común tendrá como propósito establecer un marco general de gobernanza de internet y neutralizar los efectos negativos de la revolución digital ante la amenaza de un presente *online* antidemocrático. Una unión de naciones que garantice el desarrollo democrático del futuro digital y desbloquee el florecimiento de una prosperidad compartida.

Así, la Alianza podrá hacer frente, en bloque, al modelo autoritario ruso y chino. El gigante asiático está atrayendo a su órbita a otros países con la excusa de ayudarles a construir su infraestructura digital, en el marco del proyecto de la Ruta de la Seda digital. Son al menos dieciséis países los que están ya bajo su estela, aunque se sospecha que puedan ser muchos más.[7] ¿Y si China terminase marcando las reglas de juego digitales e imponiendo su sistema de vigilancia, censura y control *online* en una amplia extensión del mundo conectado?

Si los países democráticos no logran ponerse de acuerdo, el ciberespacio podría acabar siendo un lugar diseñado para apoyar las autocracias.[8] De ahí la urgencia e importancia de la Alianza como unión de las naciones democráticas para definir las

reglas digitales; para diseñar y poner en marcha nuevas instituciones, leyes, procesos y derechos. Así pasó con la Revolución Industrial y así debe suceder con la revolución digital.

La idea de tal coalición va ganando adeptos. Propuestas hay muchas. ¿Quién debería integrarla, además de Estados Unidos y la Unión Europea? Probablemente no solo las democracias consolidadas, sino también países en desarrollo que, de ser excluidos, podrían buscar el amparo de China. Esto no sería una mala noticia si el gigante asiático estuviera dispuesto a abrir su internet, a renunciar a la censura y a hacer una transición democrática. Mientras no sea así, internet seguirá siendo una red con fronteras, aunque no serán tantas si las democracias son capaces de unirse.

Eso nos lleva a la siguiente pregunta: ¿cuál debería ser el cometido y contenido de la Alianza? Mucho está por definir y no será fácil. Este pasa inexorablemente —aunque no solo— por la regulación, ya sea adaptando la legislación actual o creando nuevas normas. La Alianza debe fijar el rumbo de la gobernanza de internet en torno a aspectos económicos y de mercado, de privacidad y datos, de justicia algorítmica, de valores, de derechos y deberes, y de infraestructura y ciberdefensa.

VALORES Y DERECHOS GUÍA

Vaya por delante que hablamos de una alianza de democracias cuyos acuerdos e iniciativas deben respetar y tener como guía la Declaración Universal de los Derechos Humanos (DUDH), de forma que se garanticen un desarrollo digital digno y dignificado y una digitalización ética, todo ello en el marco de una internet abierta y no segregada.

La regulación de la sociedad digital debe basarse en la identificación de valores individuales y sociales que se quiere proteger y, conforme a ellos, crear normas.[9] Debe centrarse en los valores humanos (justicia, equidad, solidaridad, libertad, responsabilidad, ética, respeto, tolerancia, paz, bondad, amor, amistad, honestidad…), de forma que siga vigente a medida que aparecen, se desarrollan y se consolidan nuevas tecnologías. A diferencia de estas, tales valores son innatos, perdurables y universales.

Si bien se han hecho esfuerzos integradores de voluntades a través de cartas de derechos digitales, estas resultan insuficientes o, a veces, equívocamente enfocadas. Bajo una falsa dualidad que asume que lo digital es diferente de lo real, a menudo tratan de derechos ya reconocidos en el mundo *offline* que, o bien se aplican ya, o bien deberían aplicarse a lo digital. En este sentido, lo que se necesita son mecanismos que fuercen su cumplimiento y herramientas efectivas de defensa de los derechos fundamentales que se vulneran a diario por medios tecnológicos.[10]

Una vez consensuados los principios, hay que avanzar en políticas y prácticas, y en normas que den seguridad jurídica. En algunos aspectos es posible que sea necesario ampliar derechos, deberes y protecciones para cubrir vacíos legales y

situaciones no previstas cuando no existían las tecnologías actuales o algunas de sus aplicaciones.

ZONA DE COMERCIO DIGITAL[11]

La respuesta a muchos de los problemas de gobernanza *online* puede estar en la creación de una Zona de Comercio Digital que vincule la adopción de valores democráticos en internet con el acceso a los mercados digitales. Esta Zona mantendría el libre flujo del comercio digital a través de las fronteras de los países miembros de la Alianza. Ello implicaría la implantación y el obligado cumplimiento de estándares y prácticas comunes, así como imponer aranceles sobre productos digitales de estados no miembros, además de sanciones a quienes participen en actividades prohibidas.

Esos estándares y prácticas se dirigirían a garantizar la privacidad y la no discriminación, a prevenir la desinformación, a mejorar la ciberseguridad, a fortalecer la infraestructura y a reducir la dependencia de países no miembros, entre otras cosas. Al vincular el acceso a la Zona de Comercio Digital a las obligaciones asociadas, las naciones de la Alianza pueden crear una alternativa convincente a las visiones autoritarias acerca de internet.

GOBERNANZA DE DATOS

Empecemos por los datos y la privacidad. El acuerdo para la Zona de Comercio Digital debería establecer unos principios para la protección de la privacidad y las libertades civiles y un proceso para determinar si los estados candidatos a miembros acatan esos principios. ¿Y qué mejor manera que usar el Reglamento General de Protección de Datos (RGPD) europeo para ello? Tal vez haya quien se lleve las manos a la cabeza con la propuesta, pero lo cierto es que el RGPD se ha convertido en un estándar global con el potencial de ser más unificador que divisor. De hecho, numerosos países (Brasil, India, Japón, Corea del Sur y Tailandia) se han inspirado en él para desarrollar sus leyes de protección de la privacidad.

Incluso en Estados Unidos se han creado normas bajo la influencia del RGPD, como, por ejemplo, la Ley de Privacidad del Consumidor de California. La interoperabilidad entre las leyes de las naciones democráticas a uno y otro lado del charco reduciría la complejidad del cumplimiento y los costes legales. Se evitaría así que las empresas tuvieran que construir sistemas separados para cumplir con requisitos diferentes de protección de la privacidad en los países donde operan, lo cual ya es un problema conocido para grandes y pequeñas compañías. La adopción del RGPD como norma común para los países miembros de la Alianza permitiría pasar de una situación de fricciones a otra de homogeneización de requisitos.

Sobre la base del RGPD europeo, se debe desarrollar una arquitectura multilateral sólida que refleje las reglas y valores colectivos de los estados miembros: un conjunto

universal de normas digitales y estándares para gobernar el uso de datos sin comprometer la libertad y los derechos humanos.[12] Reglas —nuevas o basadas en propuestas existentes o en la ampliación de leyes ya en aplicación, según proceda— que el grupo pueda adoptar junto con un mecanismo de aplicación para ayudar a mediar en los posibles desacuerdos entre las partes.

La tarea es compleja. Para que esas normas sean de verdad respetuosas con la libertad y los derechos humanos, hay que abordar uno de los grandes problemas de la economía digital: los modelos de negocio extractivos. Esos modelos explotan y tratan de obtener rédito económico de todas las actividades humanas comercializables *online* a través de los datos de cada usuario. Se basan en extraer y comercializar nuestros datos para brindar a los anunciantes la oportunidad de usarlos para manipularnos. Conllevan vigilancia y rastreo permanente, invasión de la intimidad y pérdida de la privacidad.

Estos modelos no cumplen con algunos de los derechos humanos fundamentales, son antidemocráticos. ¿Cómo acabar con ellos? Eliminando sus incentivos financieros y prohibiendo los mercados de datos personales.[13] Como dice Carissa Véliz en *Privacidad es poder*, ciertas cosas no tendrían que estar a la venta. Los datos personales —nuestros miedos, esperanzas, placeres, traumas, secretos, conversaciones, rutinas y datos médicos— no deberían ser algo que cualquiera puede vender, comprar o compartir a cambio de dinero.

Muchos dirán que prohibir el comercio de datos personales es una locura, que supondría cargarse una buena parte del sustento de la economía digital, pero es que ese es el problema: un modelo económico legítimo no puede sustentarse en la violación de derechos humanos. En el pasado, economías enteras se basaban en la trata, lo que no impidió que se prohibiera el comercio de personas y se aboliera la esclavitud.[14] De igual manera, que existan organizaciones dedicadas a facilitar las tareas necesarias para efectuar de forma efectiva este modelo no justifica dichas tareas.

Otra falacia es la de la calidad de producto, servicio, recomendación, etc., que se suma a la trampa de la personalización. Muchos dirán que sin recopilar nuestros datos personales y escarbar en ellos las empresas no podrán ofrecer soluciones personalizadas y, por tanto, sus productos y servicios tendrán una peor calidad, lo cual afectará negativamente a los consumidores. Eso ya no cuela: sabemos que toda esa información personal sobre nosotros que se reúne se usa como valor predictivo cuyo fin primario es manipularnos en su beneficio. El propósito no es proporcionarnos mejores experiencias o cosas que nos gustan, sino que usemos más su producto, compremos más o permanezcamos más tiempo en su plataforma. En palabras del presidente de Apple, Tim Cook:

> La tecnología no necesita grandes cantidades de datos personales de docenas de sitios web y aplicaciones para tener éxito. La publicidad existió y prosperó durante décadas sin ello. […] Si una empresa se basa en engañar a los usuarios sobre la explotación de datos, sobre

> opciones que no son opciones en absoluto, entonces no merece nuestro elogio. Merece una reforma.[15]

En realidad, hay varios componentes del modelo extractivo y canibalizador de la atención susceptibles de reforma. La publicidad es uno de ellos. Es necesario replantear su esencia y objeto.[16] ¿Qué formas de manipulación de la conducta pueden considerarse modelos de negocio aceptables? ¿A qué principios debemos sujetar los mecanismos de la persuasión comercial, sabiendo que inevitablemente se emplearán también para la persuasión política? ¿Cómo la publicidad puede servirnos mejor a todos? Son preguntas cuyas respuestas han de plantearse desde una perspectiva de la ética publicitaria. La publicidad debe ofrecernos información, no quitárnosla.[17]

Las tecnológicas se escudan en el blanco o negro. Dicen que la única alternativa al *statu quo* invasivo es el sistema anterior a internet, en el que las empresas trataban de adivinar cuál era el espacio más adecuado para anunciar cada tipo de producto, servicio, etc. Incluso si así fuera, no sería una hecatombe; hemos vivido así varios siglos y aquí estamos. La realidad, no obstante, es que es posible encontrar un punto medio eficaz, uno que permita conocer los perfiles de los consumidores y elaborar estadísticas de forma agregada —sin nombres, apellidos ni posibilidad de reidentificación— sin violar la intimidad de las personas. Ese punto medio es el que se debe exigir.

Para más inri, el modelo de negocio publicitario extractivo está construido sobre una ficción. La supuesta hiperpersonalización publicitaria a través de la microsegmentación de la que viven muchos gigantes tecnológicos y una enorme parte de las aplicaciones «gratuitas» es una burbuja. El exdirectivo de Google Tim Hwang establece en su libro *Subprime Attention Crisis* un paralelismo entre el papel de la vivienda en los mercados financieros anteriores a la crisis de 2008 y el rol de la publicidad en la economía digital.[18] Gran parte del problema tiene que ver con el intrincado y opaco proceso de la publicidad *online*, automatizado y accionado por máquinas. Esto hace difícil comprender su inutilidad.

La creciente disponibilidad y uso de opciones de bloqueo de anuncios *online* hace aún más baldío el derroche de dinero en la microsegmentación publicitaria en internet. Eso por no hablar del fraude de las granjas de clics, con miles de personas clicando en anuncios para aumentar sus tasas de (manufacturado) éxito, o de las agencias de medios que hacen pasar por un triunfo publicitario compras que los consumidores habrían hecho de todos modos.

El de la publicidad *online* microsegmentada es un círculo vicioso que hay que romper. ¿Cómo? Regular y dotar de transparencia a ese mercado es imprescindible, pero hay que ir más allá. Es necesario, como demanda el Supervisor Europeo de Protección de Datos (EDPS, por sus siglas en inglés),[19] prohibir la publicidad personalizada *online* y restringir las categorías de datos que se pueden procesar para ajustar los anuncios, buscando el punto medio en el uso de datos añadidos.

Pero hay que tener cuidado con los puntos medios, porque pueden ser engañosos. La posibilidad de orientar los anuncios *online* hacia grupos de personas con intereses similares en lugar de hacia individuos puede volverse contra los usuarios. Esa medida, aparentemente restrictiva, es la que Google dice que impondrá a los anunciantes en su buscador Chrome de aquí a 2022. Que la empresa de publicidad más grande del mundo diga que eliminará las herramientas de rastreo de terceros es, a priori, una buena noticia. Significa que, en principio, estos no podrían identificar de manera única a los usuarios de la web cuando se movieran de un sitio a otro a través de internet. Sin embargo, las herramientas que Google propone usar como alternativa proporcionarán a los rastreadores nuevos flujos de datos con los que podrían crear sus perfiles de usuario. Es el mismo perro con distinto collar.

El anuncio de Google es, a todas luces, oportunista. Una estrategia para tratar de situarse, junto con Apple, en el bando de las empresas que protegen la privacidad de los usuarios. Es una jugada maestra: hace un lavado de cara a su marca, prepara toda una nueva línea de herramientas para seguir publicando anuncios microsegmentados y acapara el poder sobre los datos. Y es que Google sí podrá acceder a ellos, pero no permitirá hacerlo a terceras partes. Es decir, el gigante de las búsquedas y otras grandes corporaciones que centralizan el acceso y recopilación de datos directos de los usuarios serán las beneficiadas, ya que con ello tendrán más poder sobre la publicidad *online*.

Ese poder, el abuso de su posición dominante y otras conductas anticompetitivas empiezan a hacer mella. Incluso en un país tan liberal en lo económico como Estados Unidos hay un apoyo generalizado, en la mayoría de los grupos de edad, niveles educativos, demografía e ideologías políticas, a una mayor regulación antimonopolio contra las grandes empresas de tecnología.**[20]** Crece el recelo hacia estas compañías, especialmente entre la generación Z.**[21]**

Tanto la Unión Europea como Estados Unidos tienen cada vez más ganas de hincarles el diente a las GAFAM. El Gobierno estadounidense ha accionado demandas históricas contra Facebook y Google por conductas monopolísticas. La Comisión Europea ya ha multado por dichos asuntos a estos y otros gigantes tecnológicos, y probablemente siga haciéndolo como resultado de múltiples investigaciones abiertas. De hecho, la Unión Europea ya planea limitar el poder de las grandes plataformas sistémicas, a las que denomina «guardianas de acceso», en su propuesta de Ley de Mercados Digitales.**[22]** En la misma línea, el Reino Unido ha creado su Unidad de Mercados Digitales (DMU, por sus siglas en inglés), una nueva entidad reguladora que se encargará de diseñar un nuevo régimen de competencia para los gigantes tecnológicos que permita ampliar opciones y control sobre sus datos a los consumidores.

¿Por qué y cómo abordar esto desde la perspectiva de la privacidad de datos? ¿Qué tiene esto que ver con la privacidad? Tiene todo que ver: los efectos de red conducen a las plataformas *online* a la concentración. La concentración reprime la

elección. Y, a falta de elección, mayor poder. Si estas empresas no tuvieran tanto poder, no les consentiríamos rastrear toda nuestra actividad en internet. Pueden hacerlo porque tienen la potestad de monopolios *de facto* para hacer algo que claramente va en contra de los intereses de los usuarios.

Alguien podrá decir que para eso están las solicitudes de consentimiento que aparecen al descargar una aplicación o al entrar en una nueva página web. «Este sitio web utiliza *cookies* para mejorar la experiencia del usuario. Al utilizar nuestro sitio web, usted acepta todas las *cookies* de acuerdo con nuestra política de *cookies*», dice una petición de consentimiento cualquiera. La transparencia brilla por su ausencia. Otras al menos explican que esas *cookies* se dedican a recoger datos que luego usarán para personalizar contenido y anuncios, y para analizar el tráfico de su página. Algunas incorporan opciones para marcar o desmarcar los datos que queremos que se recojan de nuestra actividad en la web, con un mínimo obligatorio.

El Reglamento Europeo de Privacidad Electrónica,[23] que impone que toda web debe mostrar estas solicitudes, se hizo supuestamente para garantizar el respeto de la vida privada, la confidencialidad de las comunicaciones y la protección de los datos personales *online*. Sin embargo, ha acabado haciendo todo lo contrario: facilitando que las webs puedan rastrearnos con nuestra aceptación expresa.

El consentimiento es muy a menudo papel mojado. Lo explica claramente su dimensión relacional y estadística. Incluso si no consentimos el uso de nuestros datos, una organización puede emplear los que tiene sobre otras personas para hacer extrapolaciones estadísticas que nos afecten.[24] Es decir, dependemos también del consentimiento de otros usuarios. Existen innumerables y a menudo inimaginables vínculos —directos e indirectos— entre los datos relacionados con una persona, los datos sobre esa persona y los datos inferidos sobre esa persona a través de otras personas.

Los consentimientos de *cookies*, de términos y condiciones y de políticas de privacidad están diseñados, por lo general, para aumentar su ratio de conformidad. Es decir, para que hagamos «clic» en aceptar, sin miramientos. Para eso y para molestar a los usuarios con la obligación de tener que leer decenas de documentos al día. Algo a todas luces improbable. Así que no es cierto eso de que las personas acepten la invasión de su intimidad *online* a cambio de usar el servicio en cuestión; es que no tienen más remedio que darlo para acceder a dicho servicio. No es una elección, se trata de la única opción.

Esta realidad es, cerrando el círculo, producto del poder que tienen las grandes plataformas. Y los efectos de este poder y el comportamiento de las GAFAM y otras empresas que puedan tener conductas anticompetitivas trascienden la privacidad. Compra de empresas rivales, cooptación de la innovación o fijación de precios constituyen otros problemas asociados. Las propuestas de abordamiento son diversas: desde romper en trocitos a estas empresas y deshacer algunas de sus absorciones y

adquisiciones (por ejemplo, separar Facebook e Instagram o WhatsApp, o a Google de Fitbit) hasta restringir nuevas adquisiciones.

Todas esas medidas tienen contrapartidas que pueden afectar negativamente a otras empresas, y no está claro cómo beneficiarían a los usuarios en materia de privacidad. Hay una opción alternativa que, sin embargo, podría ayudar tanto a quitarles poder a las GAFAM como a devolver a cada cual su legítimo derecho de controlar y decidir cómo, cuándo, por qué, con quién y para qué comparte sus datos. Esa medida es la «portabilidad» de los datos.

La portabilidad es un nuevo derecho introducido en el Reglamento General de Protección de Datos (RGPD) que permite a cada persona recibir, procesar y transferir sus datos personales de acuerdo con sus deseos, y administrarlos y reutilizarlos por sí misma. Esto se traduce en la posibilidad de transferir los datos personales de una cuenta a otra o de una plataforma a otras sin barreras, recibir una copia de estos en un formato que permita al usuario reutilizarlos fácilmente o transferir o recibir cualquier dato personal que haya proporcionado.

El tipo de datos que se pueden trasladar no son solo los proporcionados directamente por el usuario, sino también los generados por la actividad *online*. Por ejemplo, el historial de búsqueda *online*, las ubicaciones o —en caso de dispositivos de medición de actividad— datos como la frecuencia cardiaca. Lo que no contempla el RGPD es la posibilidad de portabilidad de los contactos de cada persona en cada plataforma: su grafo social (la red humana en torno a un individuo).

Un grafo social interoperable bajo estándares abiertos que garanticen el control de los usuarios sobre sus datos es imprescindible. También lo es tener la posibilidad de trasladar el contenido que vertimos en cada plataforma. Por ejemplo, nuestros tuits o publicaciones, o los mensajes privados en las redes sociales. Esto es posible ya en algunas. WhatsApp permite exportar chats y Telegram, importarlos, de forma que se puede trasladar el histórico de la conversación con una persona en WhatsApp y seguir aquella en Telegram, manteniendo el historial completo.

Forzar la interoperabilidad y la portabilidad de datos, del contenido (al menos de las conversaciones privadas o grupos) y del grafo social se traducirá en la posibilidad de que los usuarios se muevan fácilmente de un servicio a otro. Y qué mejor forma que esa para alentar la competencia y los mercados abiertos.

En esta misma línea, se deben desarrollar políticas de conocimiento libre y de datos abiertos, y vehiculizar la opción de permitir el acceso y uso de datos personales con fines de investigación, de generación de conocimiento o de cocreación social. Es decir, de uso de datos como parte del procomún digital. En Europa hay diversas iniciativas en esta línea que se pueden tomar como inspiración, referencia o punto de partida. Por ejemplo, DECODE,[25] nacida con el objetivo de desarrollar herramientas para la reapropiación de los datos por parte de la ciudadanía, de modo que cada persona pueda controlar si mantiene la privacidad de su información personal o la comparte por el bien público.

En el ámbito científico, una buena aproximación para esto son los principios FAIR[26] (Findable, Accessible, Interoperable, and Reusable), que requieren que los datos sean localizables, accesibles, interoperables y reutilizables. La Comisión Europea ha adoptado estos principios en su iniciativa European Open Science Cloud (EOSC) para el desarrollo de un entorno federado, virtual y fiable para almacenar, compartir, procesar y reutilizar objetos digitales de investigación (datos incluidos).

Otra propuesta europea en esta línea es TRUST (Transparency, Responsibility, User focus, Sustainability and Technology), planteada como espacio seguro de confianza para compartir datos. Tiene como objetivo desarrollar una plataforma federadora para intercambios de datos de forma segura, fiable y que cumpla con el RGPD europeo, aunque está aún en un estadio muy incipiente como para sacar conclusiones. Este tipo de iniciativas son fundamentales para aportar confianza a los usuarios a la hora de compartir datos.

Para alentar la confianza serviría también imponer un deber fiduciario a los tomadores de datos personales.[27] Es decir, que estos estén obligados a actuar en el mejor interés de los usuarios cuyos datos recogen y que se encuentran en una situación de asimetría de poder con respecto a la organización que tiene sus datos. Es un deber al que se someten ya profesionales como los psicólogos o los abogados, y que tendría sentido aplicar a quienes recopilan y usan datos personales.

Por otra parte, dicha recopilación debe ser muy cuidadosa y no ha de ser nunca la opción por defecto, como sucede ahora. Es necesario forzar a las entidades a cambiar la formulación de las solicitudes de aceptación que aparecen al visitar una web o descargar una aplicación: pasar del «Acepto que se recojan X datos para X usos» al «No acepto que se recojan X datos para X usos» como primera opción. Y, por descontado, entre esos usos no entraría en ningún caso la publicidad microsegmentada, una vez prohibida.

Es importante también obligar a quienes recogen datos a tener un plan para borrarlos,[28] u ofrecer dicha posibilidad a los usuarios a quienes les pertenezcan (salvo contadas excepciones, como los registros de nacimiento). Esto es algo que debe incluir también la Alianza, en un punto que obligue a toda organización —sin importar lo grande que sea ni su modelo de negocio— a borrar toda información recopilada de forma ilegítima.

En cuanto al daño causado por las plataformas basadas en la economía de la atención en términos de bienestar, se deberían imponer sanciones. Sería complicado entrar en matices de bienestar o cuantificar cuándo la atención prestada a una aplicación es útil o una mera distracción (podría acarrear, por ejemplo, una penalización inmerecida al entretenimiento o diatribas con respecto a qué es entretenimiento de calidad y qué no). Una medición clara es la de la adicción, que sí podría usarse para imponer sanciones a las plataformas cuando la atención se convierta en eso, en adicción.

Especialmente propensos a volverse adictos a las *apps* y redes sociales de moda son los más jóvenes. La protección de los menores como colectivo vulnerable es algo que la Alianza también debe abordar. Italia ordenó a la red social TikTok bloquear perfiles de menores de trece años tras la muerte de una niña de diez en 2021 por participar en un peligroso reto que se había popularizado en la plataforma. Ello a pesar de que la edad mínima para acceder a la popular *app* es de trece años. De hecho, en el RGPD,[29] el tratamiento de los datos personales de un niño se considera lícito hasta un mínimo de dieciséis años, salvo que sus padres o tutores lo hayan autorizado o que el país donde vivan haya fijado un límite de edad inferior.

Otros casos sonados, como la polémica violación virtual del avatar de una niña de siete años en un videojuego *online* en 2018,[30] sirven también como ejemplo de la necesidad de reforzar el cumplimiento de las reglas de conducta en plataformas *online* y de sus propios términos y condiciones, especialmente en aquellas dirigidas a los más pequeños o susceptibles de que estos participen de ellas. No se trata de criminalizar internet, ni de generar una actitud hostil hacia lo digital, ni de prohibir el acceso a la red a los menores, sino de asegurar ciertas salvaguardas frente a este tipo de riesgo.

Por último, es necesario buscar un equilibrio entre seguridad y privacidad en las actividades de vigilancia masiva de los servicios de inteligencia de cada Gobierno, que no pueden justificar violaciones indiscriminadas de la intimidad. Conviene tener en cuenta un reciente fallo del Tribunal de Justicia de la Unión Europea,[31] que prohibió al Reino Unido, Francia y Bélgica la transmisión o retención general e indiscriminada de datos de tráfico y datos de ubicación. También dictaminó que los servicios de seguridad de estos países solo podrán acceder a los datos personales de los usuarios de teléfonos e internet cuando exista una amenaza grave para la seguridad nacional. La retención debe estar limitada en el tiempo a lo estrictamente necesario, con las adecuadas y efectivas protecciones y un sistema de revisión independiente.

DESINFORMACIÓN

> En un momento de desinformación desenfrenada y teorías de la conspiración impulsadas por algoritmos, ya no podemos hacer la vista gorda […]. ¿Cuáles son las consecuencias de priorizar las teorías de la conspiración y la incitación violenta simplemente por aumentar las tasas de participación? ¿Cuáles son las consecuencias no solo de tolerar, sino también recompensar el contenido que socava la confianza del público y las vacunas que salvan vidas? ¿Cuáles son las consecuencias de ver a miles de usuarios unirse a grupos extremistas y luego perpetuar un algoritmo que recomienda aún más? Ya es hora de dejar de fingir que este enfoque no conlleva un coste —una polarización— de pérdida de confianza y, sí, de violencia.
>
> TIM COOK, director ejecutivo de Apple[32]

Como a estas alturas ya sabemos, la desinformación, la polarización y el odio son otros de los grandes quebraderos de cabeza de la gobernanza *online*. Más aún en

época de elecciones: el termómetro de tendencias de violencia e incitación en Facebook subió nada menos que un 45 por ciento[33] entre el 31 de octubre y el 5 de noviembre: justo antes, durante y justo después de las elecciones estadounidenses. Los niveles se dispararon en enero de 2021, en medio del asalto al Capitolio. Recordemos que, para frenar la escalada de violencia, Twitter y Facebook acabaron bloqueando las cuentas del presidente Trump por publicar mensajes inexactos e incendiarios. «Al final, dos multimillonarios de California hicieron lo que legiones de políticos, fiscales y agentes del poder habían intentado y no habían podido hacer durante años: desconectar al presidente Trump», ironizaba el columnista de *The New York Times* Kevin Roose[34] al respecto.

Los políticos españoles tampoco se libraron: semanas después del suceso del Capitolio, Twitter suspendió temporalmente —y por segunda vez en un año— la cuenta de Vox. En ambos casos, la plataforma dijo que el partido político había incumplido la política de Twitter sobre incitación al odio. Un mes después de aquello, Facebook congeló en su red las cuentas de personas vinculadas con el ejército de Birmania, tras protagonizar este un golpe de Estado contra el Gobierno de la Liga Nacional para la Democracia (LND).

Las medidas de la industria tecnológica para limpiar las plataformas y redes sociales de contenido potencialmente inflamable pusieron de manifiesto el riesgo de que líderes de empresas no elegidos de forma democrática ni sometidos a escrutinio público definan los límites de la libertad de expresión. ¿Acaso deben ser ellos quienes marquen las reglas del discurso público y delimiten qué es y qué no es aceptable? La pregunta no tendría sentido, o no importaría, si estas empresas no contaran con tanto poder, si no tuvieran bajo sus dominios una buena parte de la esfera pública digital. Sin embargo, lo tienen. Si quieres ser parte de la conversación *online*, has de estar ahí, por mucho que no te gusten sus reglas.

No puede ser que estas plataformas controlen quién tiene acceso a la plaza del pueblo digital, que tengan un poder comparable al de muchos estados nación y que lo ejerzan de forma arbitraria. Cierto es que detrás de esas plataformas hay corporaciones privadas con derecho a decidir y definir sus propias reglas de funcionamiento. Igual de claro está que estas no pueden ir en contra de la ley o de los derechos humanos. Si su modelo de negocio viraliza la desinformación y los mensajes de odio, al tiempo que penaliza el debate sosegado y el contenido informativo objetivo no incendiario, lo que hay que atacar es ese modelo. Poner parches, como eliminar cuentas o bloquear de forma temporal o permanente a usuarios, no soluciona el problema de base.

La autorregulación tampoco funciona. Facebook, Google, Twitter, Microsoft o TikTok son todas firmantes del Código de Prácticas sobre Desinformación puesto en marcha por la Comisión Europea,[35] por el que estas empresas se comprometen a minimizar las oportunidades de obtener dinero para los proveedores de desinformación, brindar herramientas para encontrar diversas perspectivas sobre

temas de interés público, mejorar la capacidad de los investigadores y los grupos de la sociedad civil para monitorear el alcance y la escala de la publicidad política, fomentar la formación en materia de pensamiento crítico y medios y capacidades digitales o apoyar la red de verificadores de hechos.

Algunas medidas, como la sugerencia de Twitter de leer el contenido de un enlace antes de compartirlo, caminan en la buena dirección, pero siguen sin ir al fondo del problema. Además, no basta con reducir las posibilidades de lucro para los difusores de desinformación; hay que cortarlas de raíz. El enfoque, ya planteado, de prohibir anuncios personalizados, facilitar la portabilidad de datos y del grafo social, así como alentar la competencia, puede aportar una solución más integral a esto. Ello obligaría a las plataformas a brindar un buen servicio para evitar perder a sus usuarios. De nuevo: pasar de extraer valor de las personas a aportárselo. Construir espacios saludables que fomenten la interacción cívica, con un plan para la gestión del contenido que refleje una escala más humana y que preste especial atención al contenido viral.[36]

Esto entronca con el eterno debate de si las plataformas son responsables o no del contenido que se vierte en ellas. A estas alturas, la respuesta parece obvia. Dado que se lucran con ello, deben tener obligaciones legales y reglas claras al respecto. Son tecnologías de transmisión a escala masiva y ello conlleva una enorme responsabilidad, porque los malos actores tratan sistemáticamente de usar en su beneficio los efectos de interacción entre millones de personas que buscan información. En consecuencia, más que en obligar a las plataformas a que ejerzan como moderadoras, el foco ha de ponerse en atribuirles responsabilidad legal acerca de cómo sus productos organizan, distribuyen, orientan y amplifican el contenido y los datos de otras personas.[37]

En este sentido, la Alianza podría apropiarse de las medidas planteadas en la propuesta de ley de Servicios Digitales de la Comisión Europea[38] al respecto. Entre ellas, obligar a las plataformas *online* de muy gran tamaño a evaluar —al menos una vez al año— cualquier riesgo sistémico significativo que se derive de su funcionamiento. Y entre dichos riesgos están la difusión de contenido ilícito, cualquier efecto negativo para el ejercicio de los derechos fundamentales o la manipulación del servicio —por ejemplo, mediante la explotación automatizada— con un efecto dañino real o previsible sobre la protección de la salud pública, los menores, el discurso cívico, procesos electorales o la seguridad pública.

Considerando lo anterior, las plataformas —dice la Comisión Europea— deberán aplicar medidas proporcionales y efectivas de reducción de riesgos. Aquí entran en juego los algoritmos que, de forma invisible, estructuran el funcionamiento de estas plataformas y favorecen la visibilidad de un contenido u otro. Es otra derivada de la hiperpersonalización que hay que abolir: en lugar de mostrar los contenidos más afines a cada persona o con los que se prevé una interacción y un tiempo de atención mayores en la plataforma, estos deberían asegurar el acceso a información objetiva y

la visibilidad de una pluralidad de ideas y opiniones que fomenten la discusión. Han de facilitar el ejercicio de la capacidad de ver las cosas desde la perspectiva de todos aquellos que están presentes. Solo así podremos orientarnos en un mundo común, como decía Hannah Arendt.[39] Que «nuestros cinco sentidos estrictamente privados y subjetivos y sus datos sensoriales puedan ajustarse a un mundo no subjetivo y objetivo que tenemos en común y compartimos con los demás». Y para eso debemos acceder en los mismos términos a ese mundo, sin filtros algorítmicos que nos muestren solo una parte y partes diferentes a cada cual.

Por otro lado, hay que actualizar en la era digital los parámetros de verificación propios de los códigos deontológicos del periodismo y aplicarlos en estas plataformas,[40] algo que algunas ya han empezado a hacer. Un ejemplo es la iniciativa Birdwatch de Twitter,[41] que se apoya en la comunidad de usuarios para identificar tuits que creen que son engañosos. Estos podrán añadir notas que aporten contexto en el propio tuit y calificar la calidad de las notas de otros participantes. Si hay consenso de un conjunto amplio y diverso de colaboradores, esas notas serán visibles directamente y de forma pública en los tuits.

Otro ejemplo de aprovechamiento de la comunidad para mitigar riesgos y mejorar la gobernanza de las redes sociales es el del experimento del Citizens and Technology Lab de la Universidad de Cornell, que mostró que, cuando los usuarios de la red social Reddit trabajaban juntos para promover noticias de fuentes fidedignas, el algoritmo de la plataforma comenzó, por sí mismo, a priorizar el contenido de mayor calidad.[42] Es la ventaja del dinamismo de los algoritmos.

En lo que respecta a la verificación, otro frente clave es fortalecer el periodismo y facilitar la estabilidad de los medios de comunicación como servicio crítico. En Australia, Facebook bloqueó temporalmente la opción de ver y compartir noticias a los usuarios del país en respuesta a una ley que obliga a los gigantes tecnológicos a pagar por las noticias de medios de comunicación que aparecen en sus plataformas. Google, por su parte, tiene activos acuerdos con grandes medios de comunicación en una docena de países —entre ellos Australia, Francia, Alemania, el Reino Unido y Argentina— en el marco de su iniciativa Google News Showcase, un programa de licencia de contenidos por el que paga a los medios para que seleccionen los artículos periodísticos que aparecerán en los paneles de historias de Google News y en otros de sus servicios. Una propuesta más encaminada a apoyar financieramente al periodismo de forma directa es aplicar un impuesto sobre las plataformas o sobre la publicidad digital.

En el ámbito publicitario es necesario acabar con la confusión entre información verificada y publicidad, y regular el trabajo de los llamados *influencers* para evitar publicidad encubierta. Sobre el discurso del odio y de incitación a la violencia, se habla de la necesidad de mecanismos de detección previa a su publicación, pero esto puede resultar problemático porque no siempre están claros los parámetros para identificarlo sin cruzar la delgada línea que puede separarlo de la libertad de

expresión. Esto siempre genera fricciones, como vimos con varias normas aprobadas en 2020 en España.[43]

Todo ello, en su complejidad, deberá ser objeto de consideración de la Alianza.

DISCRIMINACIÓN Y ÉTICA ALGORÍTMICA

En 2020, un tribunal neerlandés hizo historia al prohibir el sistema SyRI,[44] usado para detectar posibles fraudes a la seguridad social. El motivo: SyRI viola el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH), que protege el derecho a que se respete la vida privada y familiar. Según el tribunal, SyRI no cumple el «equilibrio justo» para poder hablar de una infracción de la vida privada suficientemente justificada. Además, el relator especial de la ONU sobre pobreza extrema y derechos humanos declaró que el uso de SyRI tiene un efecto discriminatorio y estigmatizador.

La sentencia sobre SyRI sentó un precedente contra el uso de algoritmos predictivos por parte de un Gobierno europeo. Poco después, el Tribunal de Apelación de Inglaterra y Gales dictaminó que, por el mismo motivo (violación del artículo 8 del CEDH), el uso de la tecnología de reconocimiento facial automatizado por parte de la policía galesa era ilegal. El caso había sido anteriormente desestimado por el Tribunal Superior de Justicia del Reino Unido, si bien este fijó un nuevo deber para la policía: asegurarse de forma proactiva de que estos sistemas no discriminen para evitar posibles daños antes de que sucedan.

Estas sentencias pioneras serán probablemente las primeras de muchas, dados los múltiples y crecientes usos de los sistemas automatizados de toma de decisiones, tanto en el ámbito público como en el privado. Con la ley en la mano ya se pueden abordar casos de injusticia o discriminación algorítmica, como muestra el caso de SyRI. El problema es que estas injusticias están a menudo ocultas. Para empezar, con frecuencia no somos conscientes del uso de estos sistemas en procesos que nos afectan, como puede ser una solicitud de empleo, de hipoteca o de ayudas sociales, entre otros muchos ejemplos.

De forma preventiva, algunos gobiernos locales han prohibido ya el uso de sistemas algorítmicos proclives a un mal funcionamiento, como los basados en reconocimiento facial o biometría. La ciudad de San Francisco (Estados Unidos) fue una de las pioneras: ya en 2019 prohibió por completo todo uso del *software* de reconocimiento facial por parte de la policía y otros organismos locales. Cambridge (Estados Unidos) lo hizo después, mientras que otras han impuesto moratorias. Estados como California y Washington, por su parte, han regulado algunos elementos específicos.

Varias compañías han descartado también el uso de estas tecnologías en contextos limitados. En medio del *techlash* y las protestas masivas del movimiento Black Lives Matter tras el asesinato policial de George Floyd en Estados Unidos, IBM decidió

poner fin a su *software* de reconocimiento facial para vigilancia masiva o perfilado racial. Al día siguiente, Microsoft anunció que dejaría de vender sus sistemas de identificación de rostros a los departamentos de policía de Estados Unidos hasta que el Gobierno federal regulase la tecnología. Tras las presiones, Amazon hizo lo propio: decidió suspender temporalmente el uso policial de su herramienta de reconocimiento facial (Rekognition), que ya había demostrado tener sesgos de raza y género.

La sociedad y las empresas desarrolladoras necesitan reglas claras. En Europa, el RGPD establece que el procesamiento de datos biométricos con el propósito de identificación única está prohibido. Más recientemente, la Ley de Inteligencia Artificial de la Comisión Europea prohibió la vigilancia biométrica masiva.[45] Sin embargo, existen muchas excepciones —a menudo vagas— a esta prohibición. Eso se traduce en que el RGPD aún permite el procesamiento de datos biométricos en numerosas circunstancias.[46]

La Alianza debe desarrollar un marco legal integral que restrinja cualquier almacenamiento de datos biométricos en bases de datos y que ofrezca una guía clara sobre cualquier identificación biométrica indeseable o prohibida.[47] Debe establecer normas muy precisas sobre la recopilación de datos (de acuerdo con la jurisprudencia europea de derechos humanos, la protección de datos debe comenzar en la fase inicial de recopilación para la creación de sistemas e infraestructuras biométricos)[48] y sobre su uso policial, y ser muy estricto en las pruebas de necesidad y proporcionalidad que se aplican a esos usos.

Además, como sugiere Javier de la Cueva, son necesarias normativas que regulen los tres escenarios en el proceso de datos: entrada, almacenamiento y salida. Quien proporciona, comparte o cede los datos no tiene la misma responsabilidad que quien maneja y distribuye. Hay que pensar jurídicamente en esas tres esferas. ¿Quién es responsable de los datos? ¿Quién hace la recogida y, por tanto, incluye sesgos? ¿Cuál es el sesgo dentro de los datos? ¿Cuál es la participación ciudadana en esos escenarios? Quienes tienen acceso a esos datos normalmente son grandes corporaciones, no los ciudadanos de a pie. ¿Cómo logramos la democracia con unos sistemas y tecnologías en los cuales no existe —de forma efectiva— el derecho de participación? Es necesario reformular la racionalización jurídica del poder; en este caso, de los datos.

También hay que hacer obligatorias las auditorías de precisión y no discriminación para los sistemas de toma de decisiones algorítmicas (incluidos, claro está, los de reconocimiento facial). Son necesarios tanto estándares técnicos que tengan en cuenta el sesgo y la inexactitud como pruebas de rendimiento en contextos de la vida real. También auditorías del posible impacto discriminatorio de estos sistemas a medida que se aplican, ya que incluso los sistemas más precisos serán discriminatorios si se aplican desproporcionadamente sobre ciertas comunidades. Ambos tipos de control deben practicarse de forma previa (y preventiva) a la

aplicación de estos sistemas, y de forma regular desde su momento de aplicación y durante su tiempo de uso.

Otra medida que hay que adoptar es la obligatoriedad para todos los estados miembros de la Alianza de contar con un registro abierto de algoritmos de uso público que documente el desarrollo y aplicación de sistemas automatizados en la Administración Pública, así como su uso específico y su funcionamiento. Esto es algo que ya han anunciado ciudades como Ámsterdam (Países Bajos) y Helsinki (Finlandia), y se contempla en la Estrategia Nacional de Inteligencia Artificial (ENIA) española.[49] También las empresas privadas deberán hacer públicos y fácilmente accesibles los algoritmos con alto impacto en la vida de las personas, como pueden ser las calificaciones crediticias.[50]

Garantizar el derecho a saber cuándo un proceso está mediado por un *software* que determina su resultado será también deber de la Alianza. Eso además de fijar como condición *sine qua non* para su uso que sea interpretable por parte de todos los grupos de interés a los que afecte o que vayan a usarlo. Esto, la interpretabilidad y la explicabilidad, aborda la problemática de las cajas negras. Es decir, la opaca toma de decisiones por parte de algoritmos avanzados de inteligencia artificial cuyo proceso y razones para tomar decisiones específicas no son completamente comprensibles para los humanos. Esta condición es particularmente importante para garantizar la equidad en el uso de algoritmos y para identificar posibles sesgos en los datos de base,[51] incluso si conlleva reducir la precisión o bajar el nivel de los algoritmos.

Junto con la explicabilidad, la Comisión Europea establece otros tres principios éticos para garantizar que los sistemas de inteligencia artificial se desarrollen, se desplieguen y se utilicen de manera fiable y justa: el respeto de la autonomía humana, la prevención del daño y la equidad.[52] La Alianza debe integrar estos principios y basar todo enfoque regulatorio en el respeto de los derechos fundamentales. Asimismo debe exigir la búsqueda de la máxima privacidad por diseño.

En el campo de la medición del impacto social y la ética de las plataformas *online*, otra medida fundamental es implicar a los grupos de interés en el diseño de las herramientas y en sus acciones correctivas. Además, sería interesante hacer peritaje del diseño tecnológico.[53] ¿Cuáles son los objetivos persuasivos de cada plataforma o nueva tecnología o servicio? ¿Por qué razón recomienda un vídeo y no otro? ¿Qué parámetros trata de maximizar con el tiempo de uso de cada usuario? ¿Hasta qué punto concuerdan sus objetivos con los de los usuarios que les confían su tiempo y, a menudo, su intimidad? ¿Son útiles de algún modo o una mera distracción para el usuario? ¿Cómo afectan a su bienestar? Son algunos de los aspectos que se deben evaluar.

CÓDIGOS PROFESIONALES

Antes del peritaje podrían entrar los códigos profesionales que ya rigen en otras profesiones como la médica:

> Como miembro de la profesión médica, prometo solemnemente dedicar mi vida al servicio de la humanidad; velar ante todo por la salud y el bienestar de mis pacientes; respetar la autonomía y la dignidad de mis pacientes; velar con el máximo respeto por la vida humana; no permitir que consideraciones de edad, enfermedad o incapacidad, credo, origen étnico, sexo, nacionalidad, afiliación política, raza, orientación sexual, clase social o cualquier otro factor se interpongan entre mis deberes y mis pacientes.

Es un extracto del comienzo del juramento hipocrático. Cada mención a los «pacientes» podría fácilmente sustituirse por «usuarios» y aplicarlo a programadores informáticos, diseñadores y empresarios de tecnología. Es la idea que subyace en diversas propuestas de juramento profesional o carta ética para estos colectivos. Un compromiso por un desarrollo y uso ético, justo y respetuoso con los derechos humanos de las tecnologías digitales, que considere sus posibles consecuencias indeseadas y los efectos negativos de su aplicación.

Algo parecido hicieron los ingenieros financieros Emanuel Derman y Paul Wilmott con su «The Financial Modelers' Manifesto»[54] y su correspondiente juramento, escritos en respuesta a la crisis financiera de 2007. El texto era una especie de guía ética para los «modeladores» financieros, inspirada en el *Manifiesto comunista* y el juramento hipocrático.

Siguiendo esa estela, ¿cuál debería ser el contenido del juramento para los creadores tecnológicos? Hay múltiples propuestas. Una de ellas es «The Critical Engineering Manifesto»,[55] que considera la ingeniería como «el lenguaje más transformador de nuestro tiempo, que configura nuestra manera de movernos, comunicarnos y pensar», y que «cualquier tecnología de la que se depende constituye una amenaza y una oportunidad», lo que conlleva la necesidad de estudiar y exponer sus entresijos. También sostiene que «todo trabajo de ingeniería manipula al usuario de manera directamente proporcional al grado de dependencia que produce en ese mismo usuario» y «observa que el código se expande hacia los campos de lo psicológico y lo social, al regular el comportamiento entre la gente y las máquinas con las que interactúan». De ahí la necesidad de «reconstruir las limitaciones del usuario y la acción social por medio de la arqueología digital».

JamesWilliams propone algo diferente en su «The Designers' Oath».[56] Los diseñadores son personas que «dan forma a la vida de los demás» y, como tales, deberían prometer: preocuparse genuinamente por el éxito de los usuarios; comprender sus intenciones, metas y valores de la forma más completa posible; alinear los proyectos y acciones con dichas intenciones, metas y valores; respetar la dignidad, atención y libertad de los usuarios, y nunca usar sus propias debilidades en su contra; medir el efecto total de los proyectos (en los que esté implicado el diseñador) en las vidas ajenas; comunicar de forma clara, honesta y frecuente sus

intenciones y métodos, y promover la capacidad de los demás para dirigir sus propias vidas.

Más allá del contenido, gran parte del valor de este tipo de documento deriva —como dice Williams— de su mera existencia. Es el reconocimiento de que la influencia de su trabajo en la vida de la gente es tal que precisa de algún tipo de norma ética explícita a la que ajustar la conducta del gremio.[57] Esa necesidad debe quedar recogida de alguna manera por la Alianza para, por ejemplo, formalizarlo en principios que acompañen a toda la formación profesional en los ámbitos del diseño, la programación o la gestión empresarial.

Estos gremios son cada vez más conscientes del impacto social de sus diseños y creaciones. Empieza a ser común encontrar resistencia entre los trabajadores de los gigantes tecnológicos, algunos de los cuales abandonan su trabajo por principios. Otros ni se plantean trabajar en empresas así. Y unos terceros se organizan para tratar de cambiar las cosas desde dentro, como los centenares de empleados de Google que en 2021 anunciaron la creación de un sindicato propio —Alphabet Workers Union— tras años de reivindicaciones contra «proyectos secretos de inteligencia artificial militar, discriminación, acoso y represalias».[58]

NUEVO CONTRATO SOCIAL

Hablando de derechos laborales y del impacto de la digitalización en el trabajo surgen problemas no tan modernos. Durante la Revolución Industrial en el Reino Unido (siglo XVIII) las máquinas desplazaron puestos de trabajo de forma masiva, pero no solo surgieron otros nuevos, sino que aumentó la calidad de vida. Sin embargo, los historiadores económicos aún debaten si los daños infligidos a la fuerza laboral durante aquella época valieron la pena. Para las generaciones posteriores sí, sin duda, pero para los trabajadores contemporáneos que vieron desaparecer sus medios de vida seguramente no.[59] La industrialización destruyó en su mayoría trabajos de cualificación media y las brechas salariales se dispararon. Pasó más de medio siglo hasta que el habitante medio empezó a percibir los beneficios de la Revolución Industrial.

Este tipo de fricciones se está dando igualmente ahora. La actual era de la automatización informática ha obligado a muchas personas a trabajar con salarios más bajos, o en peores condiciones, o a dejar de trabajar. También ha creado nuevos tipos de trabajo. Muchos de ellos requieren de habilidades digitales de las que carece una buena parte de los trabajadores actuales. Asumiendo que estamos en un proceso de transición similar al de la Revolución Industrial —salvando las distancias— y que nos encaminamos a un futuro mejor, es importante centrarse en minimizar los daños en el proceso. Es decir, proteger a las personas y a los colectivos más vulnerables a la digitalización y a la automatización. Se trata de garantizar una transición lo menos desigual posible y de sentar las bases para un futuro laboral que merezca la pena.

Se habla desde hace años de la necesidad de un nuevo contrato social. Como dice el experto en internet Genís Roca,[60] «tener trabajo ya no garantiza tener derechos». El contrato social del siglo XX, construido alrededor del empleo, ya no funciona para muchas y muchos. Albert Cañigueral lo recoge en su libro *El trabajo ya no es lo que era*,[61] donde constata que, si bien permanece la necesidad de unos sistemas de seguridad social nacidos para garantizar el sustento de los trabajadores cuando se enfrentaban a contingencias que les dejaban sin ingresos, estos seguros siguen anclados a una realidad desfasada del trabajo. No han evolucionado para adaptarse a su naturaleza cambiante.

En esa nueva realidad laboral,[62] los puestos a tiempo completo con los que se asocian los derechos de los trabajadores están en retroceso, las normativas laborales de concepción estatal no encajan con las nuevas formas de trabajo deslocalizado, la volatilidad de los ingresos empieza a desplazar al desempleo como el mayor reto, y aumenta la brecha de empleo digital por falta de preparación.

La Alianza debe abordar estas problemáticas en el marco de la Zona de Comercio Digital, teniendo en cuenta que, como dice Cañigueral, «cualquier sistema de seguridad es tan bueno como su eslabón más débil». Deben garantizarse para todo tipo de trabajador —independientemente de su condición— seguros de protección social con prestaciones por desempleo, por enfermedad y de asistencia sanitaria, de maternidad y paternidad, de invalidez, de vejez y supervivencia, y los relacionados con accidentes de trabajo y enfermedades profesionales.[63] Idealmente, este tipo de servicios, además de transferibles y portables,[64] serían internacionales, como sugiere Cañigueral.

También debe garantizarse un salario mínimo. Probablemente no haya un acuerdo sobre un mismo salario mínimo en todas partes, pero se podría acordar una misma base para calcularlo: lo que se conoce como «salario digno», suficiente para pagar un alquiler decente, comprar artículos de primera necesidad, etcétera. Algo complementario sería una medida similar al Ingreso Mínimo Vital español, una renta de inserción no condicionada al trabajo.

Más allá va la Renta Básica Universal, una especie de salario para todo el mundo, no condicionado a tener un trabajo. Es una medida que hay que explorar, sin que sirva como forma de «comprar la paz social»,[65] de pagar con caridad el silencio de los ciudadanos para evitar una revuelta mientras los ricos de Silicon Valley continúan enriqueciéndose y la desigualdad sigue aumentando; sin que sirva para justificar que nadie se quede atrás a la hora de disfrutar de la prosperidad digital.

Otra propuesta es la del «Ingreso de Capacitación Universal»[66] para reeducar o formar a personas cuyos trabajos se quedan desactualizados o desaparecen a lo largo de su vida laboral. Así se motivaría a las personas a seguir desarrollándose profesionalmente para adquirir las nuevas habilidades necesarias a medida que cambien las demandas laborales. Sea con este u otro tipo de medida, la Alianza debe

considerar cómo abordar tanto la recapacitación de los trabajadores como la capacitación de los aspirantes a trabajadores para roles que hace poco no existían.

Revertir la tendencia a la acumulación del beneficio en el capital en vez de en el trabajo y la redistribución de la riqueza son otros de los temas pendientes, para los cuales se pueden valorar medidas como las anteriores u otras como gravar con impuestos a los robots y a los sistemas de inteligencia artificial.

Aparte de todo esto está el derecho a la organización sindical de los trabajadores, aunque no compartan espacio ni tiempo de trabajo, y su derecho a conocer cuándo, cómo y para qué se usan sistemas automatizados de toma de decisiones en los procesos laborales y corporativos.

CIBERSEGURIDAD[67]

En el marco de la protección de la privacidad y la limitación de la vigilancia, es importante no caer en el error de países como el Reino Unido o Australia de debilitar el cifrado de las comunicaciones a escala nacional con la excusa de prevenir ciberataques. Este tipo de medida solo aumenta las invasiones de la intimidad de los ciudadanos. En lugar de crear una internet con fronteras contra los ciberatacantes, la aproximación de la Zona de Comercio Digital es la de limitar el acceso a los mercados digitales a quienes no cumplan con los mecanismos de seguridad acordados.

¿En qué deben poner el foco esos mecanismos? Esencialmente en contar con procedimientos sólidos para notificar las amenazas cibernéticas y supervisar su eliminación. Para ello sería necesario formalizar los sistemas de notificación de actividades maliciosas y hacer cumplir los requisitos para eliminar la infraestructura utilizada por los ciberatacantes. Para quienes no cooperen, el «premio» serían las sanciones. Por descontado, habría también castigos contra los malos actores que operan fuera de la zona. La Alianza debería establecer asimismo un sistema coordinado para eliminar el tráfico de empresas de fuera de la Zona de Comercio Digital que causen problemas dentro de ella.

En cuanto al espionaje, se sabe que muchos países susceptibles de ser miembros de la Alianza espían a los que serían sus aliados. Sin ir más lejos, Estados Unidos, Francia o Israel. No hay que olvidar que el estado actual de la seguridad de internet es el resultado directo de las decisiones comerciales de empresas y de las decisiones militares o de espionaje tomadas por los gobiernos.[68]

Un compromiso que hay que adquirir al respecto podría ser el de prohibir la recopilación de información de otros países mediante la interceptación de comunicaciones directas o por medios electrónicos (inteligencia de señales) y limitar el espionaje a formas más suaves de inteligencia humana. Es importante que las naciones que formen parte de la Alianza sepan que los intrusos en sus sistemas no son

otros miembros. Más allá, se les debería prohibir participar en injerencias electorales encubiertas a escala mundial, no solo contra otros estados miembros.

En materia de ciberseguridad, también será necesario un acuerdo sobre el acceso de las fuerzas de seguridad a datos cifrados y sobre el control de la venta de herramientas de ciberseguridad que puedan utilizarse tanto para probar los mecanismos de defensa como, en las manos equivocadas, para evitarlos.

Como medida adicional, se tendría que incluir algo similar al principio de defensa colectiva del artículo 5 de la Organización del Tratado del Atlántico Norte (OTAN), que compromete a todos sus miembros a protegerse unos a otros con un espíritu de solidaridad:

> Las partes convienen en que un ataque armado contra una o contra varias de ellas, acaecido en Europa o en América del Norte, se considerará como un ataque dirigido contra todas ellas y, en consecuencia, acuerdan que, si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva, reconocido por el artículo 51 de la Carta de las Naciones Unidas, asistirá a la parte o partes así atacadas, adoptando seguidamente, individualmente y de acuerdo con las otras partes, las medidas que juzgue necesario, incluso el empleo de la fuerza armada, para restablecer y mantener la seguridad en la región del Atlántico Norte.[69]

Aplicado a la Alianza Democrática por la Gobernanza Digital, el principio establecería que un ciberataque a un miembro de la Alianza se consideraría un ataque a la Alianza en su conjunto.

De igual modo que los ministros de Defensa de la OTAN acordaron en 2006 destinar un mínimo del 2 por ciento de su PIB al gasto en defensa, los miembros de la Alianza deberían también fijar un mínimo para el gasto en ciberdefensa en cada país. Pero, a diferencia de la OTAN, en este caso la directriz ha de ser obligatoria y estipular sanciones para quien no cumpla. ¿Por qué? Porque, si no, no cumplirán. De sobra es conocido el problema de la falta de incentivos y de políticas para la inversión en ciberseguridad, que se ve como un peso muerto. Asegurar la infraestructura crítica es caro, y es fácil para los responsables de las políticas descartar futuros riesgos hipotéticos.[70] Tan hipotéticos como lo era una pandemia de coronavirus en 2020.

Proteger la infraestructura esencial es otra derivada de la ciberdefensa y la ciberseguridad. De igual forma que necesitábamos tener un sistema sanitario sólido, es imprescindible proteger la red eléctrica y las telecomunicaciones, porque todo lo demás está construido sobre ellas. Una medida que se debería tomar en este sentido es alinear la fabricación de productos electrónicos esenciales y el comercio digital. Ello requeriría de planes para reemplazar los equipos fabricados en China, lo que eliminaría un riesgo significativo de las cadenas de suministro global. Para eso, la Alianza necesitaría una planificación industrial conjunta que garantizara que las tecnologías más importantes para aplicaciones de seguridad nacional se produzcan dentro de los estados miembros. Esto implicaría el apoyo de la Alianza a tecnologías y estándares abiertos que crearían un conjunto diverso de proveedores en lugar de depender solo de un puñado, como pasa hoy.

Por otra parte, debe plantearse la opción de desconectar equipos. Como bien dice el criptógrafo Bruce Schneier: «Si la única manera de proteger un equipo es no conectarlo, esta debe ser una opción válida. Hay que invertir la tendencia actual de convertirlo todo en un ordenador de propósito general, avanzando hacia una menor centralización y sistemas distribuidos, que es como se imaginó internet en primer lugar […]. Aproximadamente el 90 por ciento de la infraestructura de internet es privada. Se gestiona para optimizar los intereses financieros a corto plazo de las empresas que pueden influir en la red, no los de los usuarios o los de la seguridad de la red».[71]

INFRAESTRUCTURA DIGITAL Y SOBERANÍA NACIONAL

En términos de infraestructura digital hay que abordar varias cuestiones. Por un lado, estamos asistiendo a la mercantilización de una parte de la infraestructura básica de internet. En 2019, la Internet Society (ISOC) anunció que había acordado vender a un fondo de capital privado el Registro de Interés Público (PIR, por sus siglas en inglés). El PIR es la organización que gestiona los dominios .org, destinados desde su creación a las organizaciones sin ánimo de lucro. La noticia del paso de este bien público a manos privadas fue un jarro de agua fría para las ONG. Aquello podría traducirse en un aumento de precios de registro y renovación de los sitios web, en una reducción del gasto en la infraestructura y la seguridad subyacentes, en acuerdos para vender datos confidenciales e incluso en censura y vigilancia.

Pioneros de internet y organizaciones sin ánimo de lucro, como la Wikipedia, se movilizaron y finalmente lograron paralizar la venta. Sin embargo, la misma entidad que la canceló —la Internet Corporation for Assigned Names and Numbers (ICANN), que coordina el sistema de nombres de internet— decidió ese año (2019) permitir la subida de precios de los dominios .com, que, a diferencia de los .org, sí son comerciales, pero con restricciones relativas, precisamente, al aumento de tarifas.

Estos hechos alimentan los temores de que desaparezcan los espacios y entidades que representan el interés público en internet y, a mayores, el expolio de la infraestructura sobre la que se sustenta. La Alianza no solo deberá representar dicho interés público, sino también establecer normas claras que garanticen la participación de todas las partes interesadas en la toma de decisiones. Por ejemplo, la obligatoriedad de incluir procesos de discusión y aprobación de la comunidad ante intentos futuros de venta de los dominios .org, si fuera el caso.

Paralelamente a esta cuestión, y también relacionada con la infraestructura digital, está la dependencia de *hardware* y *software* entre países miembros y países no miembros. Europa cuenta con una buena infraestructura de telecomunicaciones y de fibra óptica, pero carece de una infraestructura competitiva para el almacenamiento de datos. Como ya hemos indicado hace varios capítulos, el 92 por ciento de los datos que se generan en Europa se guarda en Estados Unidos,[72] lo cual puede no resultar

tan altamente inconveniente si tanto los países de la Unión Europea como Estados Unidos forman parte de la Alianza.

Europa se ha puesto por fin manos a la obra y está construyendo, con años de retraso, su alternativa. Es Gaia-X, iniciativa europea para el desarrollo de una infraestructura de datos en la nube (*online*) que se pretende que sea competitiva, segura, fidedigna, abierta y transparente. Como proyecto europeo, debe ser capaz de conectarse con otros países. Su intención es sentar las bases para una infraestructura de datos abierta y federada que permita acceder a estos y compartirlos de forma segura y fiable.

La esencia de Gaia-X es la interoperabilidad. Cuenta con una lista de servicios federados a los que cualquier compañía puede unirse si cumple unos requisitos elementales, como ser capaces de operar con esta estructura federada y proporcionar datos básicos, por ejemplo el país al que pertenecen o dónde operan.[73] Estos requisitos son los filtros que los clientes podrán seleccionar a la hora de buscar proveedores.

En este contexto —en el marco de la libre circulación de datos dentro de la Zona de Comercio Digital de la Alianza—, no sería descabellado hacer de Gaia-X un proyecto global para la digitalización democrática. Considerando que Estados Unidos formaría parte de la Alianza, ello obligaría a las empresas estadounidenses —que acaparan el grueso del mercado de servicios de infraestructura en la nube a escala mundial (más del 70 por ciento[74])— a adherirse a la nube federada de Gaia-X. Y no solo eso, sino que podría contribuir a descentralizar los servicios de almacenamiento de datos, abaratando costes y reduciendo las cuotas de mercado de los grandes jugadores. Si una multitud de proveedores de la nube federados a Gaia-X entraran en juego con el reclamo de la soberanía digital, ello animaría a más naciones a unirse a la Alianza, que fortalecería su posición frente a China. Al fin y al cabo, ningún país quiere depender de otro para alojar su infraestructura esencial.

NUEVAS ARQUITECTURAS Y SOBERANÍA INDIVIDUAL

Las personas tampoco quieren depender de plataformas en las que no confían para alojar sus datos o acceder a servicios digitales. ¿Y si no tuvieran que hacerlo? Es la utopía que hace realidad una emergente familia de tecnologías que garantizan una estricta preservación de la privacidad. Algunas están ya en nuestras manos: las aplicaciones de rastreo de contactos de casos de la COVID-19 en multitud de países europeos. Estas son interoperables y pueden funcionar sin necesidad de recopilar datos personales, que se almacenan en el teléfono de cada persona y no en servidores externos. Detrás de su desarrollo tecnológico están Apple y Google, que se basaron en una nueva arquitectura de privacidad llamada DP-3T. Su creadora es, por cierto, la española Carmela Troncoso, profesora en la École Polytechnique Fédérale de Lausana y directora del SPRING Lab.

Este tipo de tecnología echa por tierra el falso paradigma de que hay que renunciar a nuestra privacidad para obtener los beneficios de nuestros datos. En contra de aquel está también Tim Berners-Lee. Su propuesta para cambiar el rumbo digital y avanzar hacia la web tal y como él la había concebido se basa tecnológicamente en el uso de *pods*, que son almacenes *online* de datos personales. La idea es que estos sirvan como una especie de caja fuerte de información donde cada persona pueda guardar y controlar sus propios datos.[75] Cada individuo podría dar acceso a sus datos a terceras partes a través de un permiso: un enlace seguro para una tarea específica, como, por ejemplo, procesar una solicitud de préstamo. De este modo, esos terceros podrían utilizar información personal de forma selectiva, pero no almacenarla.

Berners-Lee está construyendo esto sobre la base de un *software* de código abierto, Solid, como servidor web, que es una especie de gran caja fuerte digital donde se almacenan todas las cajas fuertes individuales. Al igual que en la fórmula original de la web, la idea es proporcionar estándares tecnológicos que los programadores puedan usar para crear *software* y que los empresarios puedan usar para construir sus negocios. Para vehiculizar su comercialización, Berners-Lee ha creado la empresa Inrupt, que cobra por la licencia de una versión mejorada del *software* de Solid.

Entre las empresas que ya lo están probando está la española Empathy, que usa Solid para construir un sistema descentralizado de búsqueda para sitios de comercio electrónico. Su propósito es acabar con la centralización que beneficia a las empresas con más datos (véase Amazon) para pasar de competir por la propiedad de esos datos a hacerlo por la calidad del servicio. Inrupt también tiene proyectos piloto con organizaciones como la BBC, el banco NatWest o el Servicio Británico de Salud (NHS).

Algo parecido a la propuesta de soberanía personal de BernersLee tratan de hacer en España con el proyecto Dalion. En lugar de usar cajas fuertes individuales de datos, la iniciativa española vincula la información con una especie de cartera digital donde cada persona dispone de una serie de atributos (su nombre, edad, dirección, fecha de nacimiento, estudios, etcétera) y puede permitir el acceso a cualquiera de ellos a cualquier organismo que se lo solicite. También podrá ver con quién ha compartido qué dato, pedir su eliminación o revocar permisos de uso. Todo ello a través de la tecnología blockchain.

En el terreno de las redes sociales, el primer empleado de Twitter —Evan Henshaw-Plath— ha creado una red social descentralizada «por y para las personas». Se llama Planetary y es una aplicación con un modelo abierto y distribuido basada en una tecnología llamada Scuttlebutt que permite que los mensajes se transmitan directamente entre amigos —entre pares— sin ningún servidor central. Es decir, Planetary es una red completamente descentralizada donde cada usuario —y no Planetary— gestiona sus datos y define su identidad mediante claves criptográficas.

Funciona *offline* y no tiene anuncios. Además, próximamente pondrán a disposición de los creadores de contenido herramientas para obtener recompensas por su trabajo en sus propios términos, a través de canales encriptados para cobrar por el contenido y la conexión.[76]

Henshaw-Plath está involucrado también en un proyecto cuyo excompañero, el cofundador de Twitter Jack Dorsey, apoya financieramente. Se trata de *bluesky*, cuyo propósito no es crear una red social en específico, sino un protocolo sobre el que construir toda una nueva generación de plataformas sociales (y, ya de paso, descentralizar Twitter). Persigue la creación de un estándar abierto y descentralizado para redes sociales. Lo hace, como Dalion, mediante tecnología blockchain, que permitiría el desarrollo de un modelo duradero de alojamiento, gobernanza e incluso monetización.

ECOSISTEMAS DE INNOVACIÓN DE IMPACTO

En paralelo con el trabajo de Tim Berners-Lee, otro pionero de internet lleva también unos años tratando de mejorar el estado del ciberespacio. Se trata de Ethan Zuckerman, que explora el campo de la construcción de infraestructura pública digital mediante *software* diseñado en torno a valores cívicos. En concreto, investiga cómo crear espacios *online* sin ánimo de lucro, diseñados para servir a las personas y comunidades, que puedan competir con las opciones comerciales predominantes.

Zuckerman pone de relieve la necesidad de complementar el abordamiento legislativo de las tecnologías de vigilancia con la financiación de nuevas herramientas que hagan posible vislumbrar una alternativa en la cual trabajar, en lugar de jugar constantemente a la defensiva;[77] soluciones que persigan el bien público y no solo un rápido crecimiento. Para eso es necesario invertir en la creación de redes sociales de propósito público, buscadores especializados no extractivos, nuevas tecnologías respetuosas a la hora de generar ingresos, modelos de publicidad *online* no basados en la extracción de datos íntimos, herramientas que faciliten la cocreación y la compartición solidaria de datos, y otros servicios digitales y tecnologías cívicas.

Todo ello requiere dinero. Mucho dinero. Aquí es donde entraría la Alianza, que podría crear un fondo de capital riesgo público-privado para invertir en investigaciones y en emprendimientos para la próxima generación de plataformas con valor público. Además de las contribuciones de los estados miembros, entrarían en el fondo filántropos e inversores que no buscasen únicamente la rentabilidad de sus inversiones, sino que su capital tuviera un impacto social positivo.

La comunidad de inversores tiene que enviar un mensaje al mundo: no todo vale. Algunos arrepentidos de Silicon Valley ya lo han hecho, entonando el *mea culpa* por ayudar a crear el monstruo extractivo de la vigilancia. Si además sus palabras se convierten en hechos, será una forma de desincentivar los modelos de negocio basados exclusivamente en la captura y explotación de la atención del usuario.[78]

Con estas nuevas plataformas y empresas que vayan naciendo y con otras que ya van por el buen camino, es necesario configurar un ecosistema de innovación digital que produzca valor para todos.[79] Para que ese ecosistema crezca no solo hace falta inversión y espacios de encuentro, sino medidas que incentiven los emprendimientos sociales y la transformación de las grandes corporaciones y pymes en compañías responsables. Una propuesta en este sentido es adoptar estructuras corporativas alternativas que permitan a las empresas compensar sus objetivos económicos con otros de corte social. También traducir a métricas operativas las misiones empresariales, los parámetros que definen la misión o razón de ser de cada organización.

Por otra parte, la Alianza debería premiar los desarrollos justos: visibilizar y promover el uso de las herramientas digitales respetuosas que ya existen y que sirven como alternativa a las plataformas extractivas. Un sencillo directorio podría ser suficiente. Entre las candidatas a entrar en la lista están navegadores como Brave, Firefox o Safari; buscadores como DuckDuckGo; plataformas de correo electrónico y trabajo *online* como Open-Xchange o ProtonMail; aplicaciones de mensajería instantánea como Signal; o redes sociales como Planetary. Su adopción masiva enviaría un poderoso mensaje a la industria tecnológica.

«¿Pertenecerá el futuro a las innovaciones que hacen nuestra vida mejor, más plena y más humana, o pertenecerá a esas herramientas que llaman nuestra atención para excluir todo lo demás?», se pregunta Tim Cook. Bueno, eso depende también de multimillonarios como él.[80]

IMPUESTOS

Los estados miembros deben ponerse de acuerdo sobre el régimen tributario de las grandes empresas tecnológicas, para garantizar que estas paguen sus correspondientes tributos en los países donde operan. La tasa Google, que se ha convertido en una fuente de tensiones entre los países que la aplican y Estados Unidos, es una aproximación a esto. Un ejemplo más reciente, promovido precisamente por el presidente estadounidense, es el acuerdo —alcanzado en mayo de 2021— de los países del G7 (Estados Unidos, Francia, Alemania, Italia, Reino Unido, Canadá y Japón) para imponer una tasa mínima global del 15 por ciento en el impuesto de sociedades.

También deben explorarse otras formas de redistribución de la enorme riqueza acumulada en manos de unos pocos. Como subraya la economista Mariana Mazzucato, los gigantes digitales se están beneficiando de tecnologías que fueron financiadas por los contribuyentes, que proporcionaron las tecnologías subyacentes clave. Hay que reconocer que el valor económico se crea colectivamente y establecer asociaciones más simbióticas entre las instituciones públicas y privadas y la sociedad civil.[81]

MEDIO AMBIENTE

El coste medioambiental de internet y de las empresas de tecnología altamente demandantes de energía podría requerir asimismo de un impuesto. Microsoft se ha comprometido a tener emisiones de carbono negativas en 2030 y a usar únicamente energías renovables para abastecer todos sus centros de datos, sus edificios y sus campus. Esto podría convertirse en una obligación generalizada para todas las organizaciones que hacen un uso intensivo de energía en el contexto digital. Y, para quien no cumpla, en un impuesto que grave su desfase.

Otra solución podría ser extender a las empresas de datos la Directiva (europea) sobre las Emisiones Industriales (DEI).[82] Esta define las obligaciones de las grandes instalaciones industriales para evitar o minimizar las emisiones contaminantes a la atmósfera, al agua y al suelo. La DEI exige que las industrias reduzcan la generación de residuos, establece límites de emisión aplicables a toda la Unión Europea en relación con determinados contaminantes e introduce requisitos mínimos referentes a la inspección. Otras medidas se encaminan a proporcionar incentivos para la innovación ecológica y a apoyar la creación de mercados de vanguardia.

Incluyendo en la DEI a las industrias tecnológicas altamente contaminantes, se podría estimular una transición similar a la de la industria de la automoción hacia la producción de vehículos ecológicos y de bajas emisiones o de emisiones cero. De igual manera, la industria tecnológica debe dirigirse hacia la producción y oferta de bienes y servicios basados en energías limpias.

A lo anterior se añadiría la prohibición de la obsolescencia programada y el apoyo al diseño de los dispositivos electrónicos para facilitar su reparación.

TRASLACIÓN NACIONAL

Las medidas tomadas en el marco de la Alianza deben ser adaptadas y adoptadas a escala nacional y local. Los gobiernos de cada país miembro se encargarán de trasladar las normas y de hacer efectivas las decisiones de la Alianza. También se requerirán por su parte planes específicos y ambiciosos de alfabetización digital y de capacitación tecnológica para estimular un buen uso de la tecnología y el aprovechamiento de las oportunidades que ofrece. Las naciones deberán asimismo atajar los problemas más urgentes de la digitalización mientras se configuran los acuerdos y normas de la Alianza.

Otra tarea para los gobiernos —a escala estatal, autonómica y local— es la canalización efectiva de la inteligencia colectiva para resolver problemas públicos y de la participación ciudadana como la plasmación del derecho cívico de contribuir a la gobernanza. Ello debe hacerse por medio de sistemas de corresponsabilidad y participación organizados, transparentes, auditables, usables, eficaces y vinculantes; el derecho al reconocimiento y trazabilidad de las contribuciones, y a la protección efectiva de las y los «alertadores» de abusos que afectan al interés general.[83]

Además, los países miembros deberían valorar crear plataformas sociales públicas con funciones análogas a las de la radio y televisión públicas, considerando que estas son esenciales para la información ciudadana (interés público) y para el debate (esfera pública). La tasa Google —o similar— podría usarse para financiarlas con dinero público, como se hace ya en España con Radiotelevisión Española (RTVE).[84]

UN POCO DE REALPOLITIK

Llegados hasta aquí, sería naíf pensar que no habrá colisiones ni contrapartidas, o que todo lo anterior no requerirá de sacrificios. ¡Un poco de realismo político, por favor! ¿Por qué tendría Estados Unidos que ser promotor o, al menos, parte central de una Alianza con la que tiene aparentemente tanto que perder? Si todas las medidas se dirigen a avanzar hacia un modelo europeo de internet basado en derechos, y ello implica que las empresas estadounidenses tendrán que pagar más impuestos (también en suelo norteamericano), ¿qué gana Estados Unidos?

Sería muy fácil —y simplista— ver esta propuesta como una jugada de los europeos para tratar de mantener a Estados Unidos a raya. Sin embargo, esos impuestos se pagarían también en suelo estadounidense. Además, homogeneizar las reglas de juego en toda la Zona de Comercio Digital, asegurando un mercado único en todas las democracias, facilitaría mucho las cosas a la industria tecnológica y acabaría con la inseguridad jurídica de tener que lidiar con decenas de mercados diferentes con distintas normas. Asimismo, y sobre todo, está el hecho de que Estados Unidos necesita más que nunca aliados para mantener su liderazgo frente a China como potencia en ascenso. En el marco de la Alianza, podrá establecer los estándares y reglas para el comercio digital y ayudar a proteger su seguridad. Al igual que se hizo en Bretton Woods y con la OTAN, la Alianza proporciona a los valores democráticos su mejor oportunidad de supervivencia, y puede traer consigo una nueva era dorada de prosperidad.

¿Y qué hay de la Unión Europea? Parece que gana mucho y no pierde nada. Pero en realidad sí pierde. Pierde excusas. Europa, salvo contadísimas excepciones, como Spotify, no ha alumbrado grandes empresas digitales, pero siempre ha podido señalar como causa la laxitud de la regulación estadounidense. La creación de la Alianza igualaría el terreno de juego y obligaría a Europa a dar un paso adelante si quiere crear sus propias historias de éxito digitales. No le quedarán excusas, pero sí lamentos: «¡Mierda! ¡Ahora son nuestros valores y todavía nos están ganando!».

PUNTO DE PARTIDA

Nadie dijo que fuera fácil, pero, a pesar de todo, muchos preferirán un mundo en el que los acuerdos y las prácticas internacionales representen los valores e intereses democráticos en lugar de los autocráticos. El ideal de una internet completamente

libre y abierta seguirá aún teniendo barreras como la Gran Muralla digital china, pero sería —o será— más libre y abierta que hoy.

Todo lo anterior es susceptible de debate, mejora, ampliación y cambio. Es un punto de partida desde el que empezar a tejer. Las medidas propuestas pretenden servir de orientación, y pueden abordarse a partir de nuevas normas o adaptando la legislación existente, según el caso.

Si bien esta no es una proposición unipersonal —dado que recoge múltiples perspectivas—, debe ser enriquecida. Esta voluntad integradora ha de guiar las decisiones de la Alianza (o comoquiera que se llame la entidad en caso de ser constituida), incluyendo en el proceso a la sociedad civil y a los grupos de usuarios, a las organizaciones sin ánimo de lucro, al mundo académico y a la industria tecnológica (adoptando medidas de contención para evitar que los poderosos lobistas de las grandes empresas de tecnología acaben marcando las reglas).

Incluir a todas las partes interesadas es crucial. Además, es necesaria una regulación dinámica. La Alianza debe estar en permanente vigilancia para actualizar las medidas tomadas y ayudar a coordinar respuestas dispares a las amenazas y oportunidades digitales que se avecinen. Como medida adicional, debería contar con un grupo independiente de observadores objetivos e imparciales que puedan fiscalizar su trabajo y ver hacia dónde se dirige el desarrollo del mundo digital.

CUIDAR DEL TODO

A su vez, las acciones de la Alianza han de ser consideradas dentro de un todo: deben encajar en el cuadro completo de bienestar planetario junto a otras luchas, como las que combaten la desigualdad, la discriminación y la pobreza o el cambio climático.

Además, sería muy miope caer en el «tecnosolucionismo», cuando lo que nos trae hasta aquí no es internet en sí misma ni la tecnología, sino esta como espejo de la condición humana y su efecto amplificador de lo mejor y lo peor del *Homo sapiens*. El odio, la violencia y el crimen seguirán reproduciéndose *online*; la polarización y la desinformación seguirán amplificándose; la discriminación seguirá perpetuándose en los algoritmos; la vigilancia seguirá abriéndose hueco a cada paso analógico o virtual que demos.

Las acciones de la Alianza pueden ayudar a la contención y a revertir progresivamente los efectos negativos de la amplificación humana, pero el cambio profundo solo se dará si construimos mejores sociedades —más inclusivas y equitativas— y democracias más participativas y transparentes. Solo sucederá si ponemos todo nuestro empeño en educar a mejores personas, sin perder de vista ni un momento los valores guía.

El centro de todo no puede ser la tecnología, ni ésta nos convertirá en *Homo Deus*. Al contrario, nos dejará un inmenso vacío. Si perdemos internet, ¿qué tenemos? Dependemos tanto y para tanto de la red de redes que apenas podemos responder. Nos quedamos sin soporte. Sin embargo, este nunca fue real. Los

verdaderos cimientos son las conexiones humanas. Si construimos el edificio sin ellos, todo saldrá mal. Porque, cuando todo falle, solo permanecerá el sustento humano como bote salvavidas.[85] Ese es el pilar que hay que reforzar.

Llegados a este punto, no hay vuelta atrás. Ha comenzado el principio del fin. El principio del fin de la internet en la que no nos queremos mirar, del capitalismo irresponsable de los modelos extractivos, del mercantilismo de lo *online,* de la renuncia a la libertad y de la pérdida de humanidad. Como decía Arendt, «todo fin de la historia también contiene un nuevo comienzo». Es hora de mirar al futuro bajo la promesa de libertad, armonía, prosperidad y florecimiento humanos. En busca —y cada vez más cerca— del nuevo amanecer.

Epílogo

Un billón de segundos

La utopía está en el horizonte. Camino dos pasos, ella se aleja dos pasos y el horizonte se corre diez pasos más allá. Entonces, ¿para qué sirve la utopía? Para eso, sirve para caminar.

EDUARDO GALEANO

Treinta y dos años son muchos: más de un tercio de la vida de cualquier persona promedio. El tiempo de descuento —preciado y precioso— para salvar al planeta del cambio climático. Treinta y dos años son muchos. ¿Son muchos? Nada comparado con los más de cuatro mil quinientos millones de años de la Tierra. Treinta y dos años son muchos o apenas nada, dependiendo de con qué los comparemos. Para internet, a sus casi cincuenta años de edad, son más de media vida. Tiempo más que suficiente para cambiarlo por completo.

Treinta y dos años son un billón de segundos. Imaginados en términos de tiempo, vida y atención —en lugar de, como suele hacerse, en forma de dinero—, permiten pensar a largo plazo y a gran escala, abriendo puertas a las mentalidades y enfoques, y a estrategias creativas para el cambio sistémico. Con esa premisa nació, en un rincón en la ciudad de Barcelona y con pequeños nodos repartidos por el mundo, The Billion Seconds Institute.

Esta es una iniciativa sin ánimo de lucro creada por los intrépidos Lucy Black-Swan y Andrés Colmenares, fundadores del laboratorio de investigación creativa IAM (Internet Age Media). Buscan organizar una red de especialistas y comunidades en aprendizaje permanente para reinventar cómo entendemos y damos forma a los impactos mentales, sociales y ambientales de la economía digital. Su objetivo: expandir y activar formas de pensar holísticas para hoy, mañana y el próximo billón de segundos.

Colmenares y Black-Swan se plantean: «¿Qué pasa si nos unimos para reinventar internet como red sostenible de conocimiento, solidaridad y cuidado?». Quieren contribuir a una transición del individualismo de una economía digital, centrada en el usuario, a la interdependencia de los ecosistemas digitales, impulsada por ciudadanos responsables del planeta Tierra. Junto con ello, un cambio de paradigma: de usuarios a interciudadanos. Interciudadanos de un espacio metafórico con bibliotecas, cafés, espacios abiertos y espacios privados.

En treinta y dos años, cuando el reloj de The Billion Seconds Institute se haya parado, sus creadores esperan que se hayan dado las condiciones para que la economía digital evolucione; que haya pasado del modelo extractivo a ecosistemas donde la distribución de valor sea más equitativa, plural, sostenible y consciente. No buscan una respuesta, sino muchas al mismo tiempo. Pasar de la noción de «progreso y crecimiento eterno» a buscar la armonía entre el desarrollo de nuestra civilización y el resto. Todo ello poniéndolo a cocer a fuego lento.

EDAD DE ORO

Colmenares y Black-Swan van a darlo todo por facilitar la transición hacia ese desarrollo armónico. No están solos. La comunidad de IAM les sigue en su propósito, y como IAM muchas más. Miles, millones de personas en muchos ámbitos, puestos, sectores y roles cuyas acciones marcarán los futuros de internet, igual que su presente lo han marcado las acciones y omisiones humanas pasadas.

La apuesta de todos esos individuos y colectivos, de ciudadanos, trabajadores, ejecutivos, legisladores, funcionarios, académicos, activistas, periodistas y autores —entre ellos quien firma este libro—, es la de hacer posible una nueva era dorada para la humanidad. Ese momento de esplendor nos aguarda ya, y está preparado para nosotros. La célebre economista Carlota Pérez, conocida por su teoría de los ciclos de las revoluciones tecnológicas,[1] asegura que nos acercamos al final del punto de inflexión de la quinta revolución, la de la información, que se producirá después del colapso social, climático, económico, ético y de valores que vivimos.

Pérez dice que estamos a las puertas de una nueva edad de oro.[2] Cada era dorada en cada revolución se produce, según su teoría, tras un periodo de recesión. El periodo actual de la revolución de la información —propiciada por los avances en tecnologías de la información y las comunicaciones, las TIC— comenzó en los años setenta, con el nacimiento de internet, el abaratamiento de la microelectrónica, el desarrollo de los ordenadores personales y la bioinformática, y de una infraestructura de telecomunicaciones mundial. Tuvo su burbuja (la de las .com) en la década del 2000 y su consecuente recesión con la crisis mundial de 2008.

Sin embargo, esta revolución es diferente. No es una, sino dos. No lo es solo de las TIC y de la información, sino de los datos masivos y la inteligencia artificial. La eclosión de esta segunda ola de desarrollo tecnológico basado en el análisis masivo de datos y la IA se ha dado paralelamente a la recesión de las TIC y no ha dejado paso al desarrollo de la fase posterior que, siguiendo la teoría de Pérez, es la era dorada. Su consecución se vio interrumpida primero por la IA, una tecnología con potencial tanto de multiplicar su efecto como de neutralizarlo, y, más adelante, por un elemento inesperado y disruptor, la pandemia mundial de la COVID-19.

La doble revolución de nuestro tiempo está en un periodo de transición de la fase de instalación de la IA a la fase del despliegue y de regulación. La recuperación está

empezando a ponerse en marcha, pero la llegada de los días de gloria no está garantizada. Solo sucederá si hay una ganancia segura y real para todos, si se direccionan los avances para el beneficio y la paz social. Hace falta voluntad para alcanzar la sociedad mundial del conocimiento sostenible que augura Pérez.

Hay señales que indican que vamos camino de ello. Junto con el *techlash* tecnológico regresa con fuerza la idea del capitalismo *stakeholder*, orientado a servir los intereses de todos —clientes, proveedores, empleados, comunidades locales, etc. — y no solo de los accionistas. Un modelo que busca alinear las metas e incentivos corporativos con los de sus grupos de interés. Al fin y al cabo, la cultura del «muévete rápido y rompe cosas» resulta no ser tan beneficiosa como parece para las corporaciones.[3]

The Economist habla de la necesidad de arreglar el roto capitalismo y de remoralizar a la clase dominante. Movimientos en todo el mundo trabajan por un modelo económico más humano, equitativo, responsable y sostenible o circular. Uno que no solo tenga como principal indicador el producto interior bruto (PIB), sino que incluya mediciones de satisfacción, bienestar y esperanza de vida saludable; que considere la desigualdad y que se fije en la riqueza en lugar de en la renta.

Si los objetivos económicos cambian, las tecnologías lo harán también. Los inversores están cada vez más preocupados por las consecuencias ambientales, sociales y de gobernanza de sus decisiones de inversión.[4] Los menores de treinta y cinco años tienen el doble de probabilidades de vender una acción si consideran que una empresa es ambiental o socialmente insostenible.[5] Es una muestra de que las nuevas generaciones buscan algo más que un rendimiento financiero.

Las empresas dominantes siguen siendo poderosas, pero la era del «todo para el ganador» («The winner takes it all», que cantaba Abba) se está desvaneciendo, a medida que la tecnología entra en una nueva fase más competitiva.[6] Nuevas plataformas emergen en y desde Silicon Valley para el mundo, mientras actores regionales o específicos de cada país desafían a los gigantes tecnológicos. Las nuevas alternativas amplían la oferta y activan la competitividad, aunque a menudo —de momento— sean más de lo mismo.

CONSTRUIR EL FUTURO

El futuro y los futuros posibles no necesitan bolas de cristal ni gurús que pretendan predecirlos. Necesitan imaginación colectiva; ser inventados y narrados. En un momento en el que sobran imaginarios distópicos, es más indispensable que nunca concebir alternativas y, por qué no, utopías que nos permitan avanzar. Que nos faciliten, como dicen en IAM, seguir adelante con esperanza de que el mañana será mejor.

Para construir, primero hay que conocer, entender y analizar. Realizar un profundo diagnóstico de situación. Es lo que hemos tratado de hacer —ustedes al leer

y yo al escribir— a lo largo de este libro:

- Hemos aprendido múltiples formas en las que podría caerse —o ser derribado— internet, lo dependientes que somos de la red de redes y el caos que un apagón podría desatar.
- Hemos conocido a los guardianes de internet.
- Nos hemos sumergido en el lado más oscuro del ciberespacio y hemos visto lo fácil que puede ser un ciberataque.
- Hemos observado cómo internet, la conectividad o el *smartphone* generan adicción a través de la economía de la atención.
- Hemos descubierto quién convirtió el beicon con huevos en el desayuno estadounidense por excelencia y qué tiene eso que ver con la manipulación.
- Hemos reflexionado sobre la desinformación, la fragmentación epistemológica y el discurso del odio *online*.
- Nos hemos indignado con las múltiples —y a menudo ocultas— formas de discriminación algorítmica.
- Hemos comprobado cómo George Orwell y Aldous Huxley se dan la mano en el siglo XXI a través de una renovada tiranía digital.
- Hemos analizado cómo hemos llegado hasta aquí.
- Hemos constatado las promesas rotas en torno a la tecnología y el pecado original de internet, cada vez más *splinternet*.
- Hemos profundizado en las consecuencias del desproporcionado poder de la industria tecnológica y la privatización de la gobernanza.
- Hemos comprobado la huella de carbono de internet, los datos masivos y la inteligencia artificial; y también su impacto en la soledad y en la cohesión social.
- Nos hemos sorprendido al descubrir cómo unos jovenzuelos nada inocentes pueden desestabilizar el mercado financiero.
- Hemos comprendido cómo internet facilita la organización social, la movilización de las comunidades o la tecnología cívica, y nos hemos emocionado y enorgullecido por ello.
- Hemos profundizado en la complejidad de abordar todos los problemas anteriores y hemos indagado en algunas posibles vías para afrontarlos, siempre con los derechos humanos marcando el camino. Y, pese a la dificultad, nos hemos ilusionado con ello.

Ahora que sabemos todo lo anterior, es nuestro deber transmitirlo. ¡Vayan y difundan la palabra! Hay que concienciar, acercar ese conocimiento a otras personas, ayudarlas a entender también; fomentar el pensamiento crítico y abrir conversaciones y debates.

Hay asimismo que seguir explorando buenas prácticas. Algunas de ellas aparecen en este libro, pero hay muchas más ahí fuera. Es necesario visibilizarlas e imitarlas. Los nuevos relatos también. Con ellas una —o uno— se puede encontrar a gusto y quedárselas, o seguir insatisfecha e imaginar otras nuevas.

Por último, hay que accionar esos nuevos relatos y visiones de futuro: planificar cómo hacer que pasen y actuar al respecto.

¿Merecerá la pena? Los futuros, parafraseando a Albert Cañigueral,[7] o los construyes o te los construyen. Hasta ahora, nos los han construido, y parece que el resultado solo ha sido bueno para unos pocos. Con lo enriquecedor, retador, divertido y apasionante que es participar en su creación, ¿cómo perdérselo? ¿Y por qué no creérselo? Solo por eso ya habrá compensado el esfuerzo.

Los potenciales futuros están al alcance de nuestra mano. El nuevo amanecer de internet, y de la humanidad, también.

Agradecimientos

Este es mi primer libro en solitario, así que perdónenme que me explaye con las dedicatorias y agradecimientos.

A mis padres, Juan Carlos e Inma, por abrirme las puertas de la vida cuando llegué sin llamar; por educarme en valores; por enseñarme a pensar, a tener una mirada crítica y a valorar las cosas importantes de la vida; por introducirme en la educación musical como experiencia vital; por acercarme al apasionante mundo de la literatura, que de forma natural me llevaría a la escritura y al periodismo; por acercarme a «internet» en la época del 486; por darme la oportunidad de viajar; por ayudarme a crecer y por dejarme volar. Gracias por todo, por ser mis primeros lectores y críticos y mis fieles seguidores.

A mi adorado Ollie, mi compañero de vida, por su sonrisa eterna, por su amor incondicional y por aportar tanto a este libro. Gracias por tus sugerencias e ideas brillantes, por cuestionarme y por retarme: por sacar lo mejor de mí. «Great minds think alike, though fools seldom differ.»

A mi abuelo Antonio, por transmitirme el valor de la nobleza y la humildad. A mi abuela Rafaela, que en paz descanse, por enseñarme a pescar. A mi difunto abuelo Gregorio por su generosidad.

A mi hermanito Manuel, que desde la distancia me alegra cada mañana, sin saberlo.

A mis tías, tíos y padrinos, por ser los mejores hermanos mayores.

A Toni, por hacerme llegar la inspiración y alentarme a escribir. Si no hubieras prendido esa mecha, hoy no estaríamos aquí.

A Andreu, por tu magia y por «liarme» hace ya ocho años para formar parte de esa gran comunidad llamada IP.

A R. P., que sabe lo mucho que aprecio su acompañamiento.

A mis amigas y amigos, de «Tururú» a los «Lovers», pasando por los «Shakers», mi querida «crazycabra», y las y los versos sueltos a quienes he conocido en diferentes etapas vitales y con quienes tengo la dicha de contar. Gracias por estar ahí.

A todas esas personas que han pasado por mi vida dejando huella.

A mis fuentes: todas aquellas y aquellos que me han regalado su tiempo, conocimiento y reflexiones y que me han permitido aprender tanto a lo largo de estos años ejerciendo el periodismo. Gracias en especial a todas las personas cuyas aportaciones han sido tan relevantes para este libro. Como dice Sinan Aral en *The Hype Machine*: «Ninguna empresa intelectual se logra en solitario». Somos pensadores sociales. Bebemos de las inspiraciones, influencias y enseñanzas de otros, de experiencias colectivas, de conversaciones y desafíos a nuestra forma de pensar y de ver el mundo, de las artes, del amor.

A mis editores, Miguel y Roberta, a quienes agradezco infinitamente la oportunidad de ver publicado —de tocar y de oler— este libro. Gracias por recibirlo con los brazos abiertos y por hacerlo posible.

A mis otros editores, los de los medios de comunicación, por contar conmigo, por valorar mi trabajo y por permitirme llegar a millones de personas. Gracias especiales a quienes me acompañaron en mis comienzos, por enseñarme tanto y dejarme hacer; a quienes confiaron en mí para sacar adelante sus proyectos; a quienes me ofrecieron un cambio de rumbo; a quienes me pagaron por divertirme; a quienes me permitieron madurar profesionalmente. Os aprecio y respeto.

A «mis Pablos», mis inseparables de la tele. No sois grandes, sois inmensos (mi querido «mono», sé que allá donde estés me estarás leyendo).

A mis buenas profesoras y profesores del I. E. S. José Hierro de Getafe, a quienes recuerdo con tremendo cariño. También a muchas y muchos maestros de la Universidad Rey Juan Carlos y de la Universidad Complutense de Madrid, cuyas enseñanzas permanecen.

A todas y todos, GRACIAS, de corazón.

Apéndice 1

Relación de propuestas del capítulo 11

Tema	Propuesta
Geopolítica de internet y cibergobernanza	Creación de un frente democrático común contra el modelo autoritario: la Alianza Democrática por la Gobernanza Digital.
Valores y derechos	• Preservación de la Declaración Universal de los Derechos Humanos (DUDH) en el contexto digital: herramientas efectivas de defensa y refuerzo de su cumplimiento. • Identificación de valores guía. • Desarrollo de normas para cubrir vacíos legales y dar seguridad jurídica.
Comercio	• Creación de una Zona de Comercio Digital que vincule la adopción de valores democráticos en internet con el acceso a los mercados digitales. • Estándares y prácticas comunes para garantizar la privacidad y la no discriminación, prevenir la desinformación, mejorar la ciberseguridad, fortalecer la infraestructura, reducir la dependencia de países no miembros...
Gobernanza de datos, privacidad y monopolios	• Reglamento General de Protección de Datos (RGPD) ampliado: una arquitectura multilateral sólida que refleje las reglas y valores colectivos de los estados miembros. Un conjunto universal de normas digitales y estándares.junto con un mecanismo de aplicación. • Prohibir los mercados de datos personales.
Gobernanza de datos, privacidad y monopolios	• Replantear la esencia y objeto de la publicidad desde una perspectiva ética: encontrar un término medio sobre qué modelos de negocio son aceptables. • Prohibir la publicidad personalizada *online* y restringir las categorías de datos que se pueden procesar. • Un nuevo régimen de competencia para los gigantes tecnológicos: retuerzo del cumplimiento de las leyes antimonopolio y limites a su poder. • Portabilidad de datos y contactos como piedra angular la posibilidad no solo de controlar y administrar la propia información, sino también de trasladar contenido y contactos de una plataforma a otra. • Políticas de conocimiento libre y datos abiertos. Ejemplos: DECODE, EOSC, TRUST. • Deber fiduciario para los tomadores de datos personales. • Evitar la recopilación de datos por defecto y obligar a la eliminación de datos e información recogidos de forma ilegítima. • Sanciones para las plataformas y redes sociales en casos de adicción. • Protección de menores: salvaguardas que protejan sin coartar su libertad ni criminalizar internet. • Equilibrio entre la seguridad nacional y la privacidad: solo acceder a datos personales de los usuarios cuando exista una amenaza grave para la seguridad nacional, de forma temporalmente limitada, con protecciones efectivas y revisión independiente.

Desinformación y discurso del odio	• Construir espacios saludables que fomenten la interacción cívica. • Aprovechar la comunidad para la mitigación de riesgos y mejorar la gobernanta de bs redes sociales. • Planes de gestión del contenido que reflejen una escala más humana y que presten especial atención al contenido viral.
Desinformación y discurso del odio	• Asegurar el acceso a información objetiva y la visibilidad de una pluralidad de ideas y opiniones que impulsen el debate. • Atribuir a las plataformas la responsabilidad legal de cómo sus productos organizan, distribuyen, orientan y amplifican el contenido y los datos de otras personas. • Adoptar o inspirarse en las medidas previstas en la propuesta de ley de Servicios Digitales de la Comisión Europea. • Actualizar los parámetros de verificación propios de los códigos deontológicos del periodismo y aplicarles en estas plataformas. • Facilitar la estabilidad de los medios de comunicación como servicio crucial con apoyo financiero directo. Por ejemplo, mediante un impuesto directo sobre las plataformas o sobre la publicidad digital. • Acabar con la contusión entre información verificada y publicidad, y regular el trabajo de los llamados *mflueníers* para evitar publicidad encubierta.
Discriminación	• Prohibición del uso de algoritmos con efecto discriminatorio y estigmatizador, incluidas las tecnologías de reconocimiento facial. • Marco legal integral que restrinja cualquier almacenamiento de datos biométricos en bases de datos y que ofrezca una guía clara sobre cualquier identificación biométrica indeseable o prohibida. (Debe ser muy estricto en las pruebas de necesidad y proporcionalidad que se aplican a esos usos.) • Normativas que regulen los tres escenarios en el proceso de datos: entrada, almacenamiento y salida. Reformular la racionalización jurídica del poder de los datos. • Auditorías previas obligatorias de precisión y no discriminación para los sistemas de toma de decisiones algorítmicas. • Auditorías del posible impacto discriminatorio de estos sistemas a medida que se aplican.
Discriminación	• Estándares técnicos que tengan en cuenta el sesgo y la inexactitud,como pruebas de rendimiento en contextos de la vida real • Registro abierto de algoritmos de uso público que documente el desarrollo y aplicación de sistemas automatizados en la Administración Pública. • Garantizar el derecho a saber cuándo un proceso está mediado por un *software* que determina su resultado,y que dicho *software* sea interpretable por parte de todos los grupos de interés a los que afecte o que vayan a usarlo. • Principios de privacidad y no discriminación por diseña • Peritación del diseño tecnológico.
Deontología	Códigos profesionales que acompañen a toda formación profesional en los ámbitos del diseño tecnológico, la programación o la gestión empresarial, en reconocimiento de la influencia de su trabajo en la vida de la gente. Una norma ética explícita a la que ajustar la conducta del gremio.

Trabajo y nuevo contrato social	• Seguros de protección social con prestaciones por desempleo, por enfermedad y de asistencia sanitaria, de maternidad y paternidad, de invalidez, de vejez y supervivencia, así como aquellas relacionadas con accidentes de trabajo y enfermedades profesionales para todo tipo de trabajador. • Idealmente, este tipo de servicios, además de transferibles y portables, serían internacionales. • Garantizar un salario mínimo, con una misma base para calcularlo. • Ingreso de Capacitación Universal para reeducar o formar a personas cuyos trabajos se quedan desactualizados o desaparecen a lo largo de su vida laboral • Explorar medidas como Renta Básica Universal, con sus pros y contras. • Revertir la tendencia de beneficio para el capital en lugar de para el trabajo.
Trabajo y nuevo contrato social.	Derecho de los trabajadores a saber cuándo,cómo y para qué se usan sistemas automatizados de toma de decisiones en los procesos laborales y corporativos.
Ciberseguridad	• Procedimientos sólidos para notificar las amenazas cibernéticas y supervisar su eliminación. • Prohibir la recopilación de información de otros países mediante la interceptación de comunicaciones directas o por medios electrónicos y limitar el espionaje a formas mis suaves de inteligencia humana. • Prohibir participar en inferencias electorales encubiertas a escala mundial no solo contra otros estados miembros. • Acuerdo sobre el acceso de las fuerzas de seguridad a datos cifrados y sobre el control de la venta de herramientas de ciberseguridad. • Principio de defensa colectiva: un ciberataque a un miembro de la Alianza se considera un ataque a la Alianza en su conjunta • Fijar un mínimo para el gasto en ciberdefensa en cada país. • Proteger la infraestructura crítica mediante una planificación industrial conjunta que garantice que las tecnologías más importantes para las aplicaciones de seguridad nacional se produzcan dentro de los estados miembros. • Apoyo a tecnologías y estándares abiertos que creen un conjunto variado de proveedores. • Desconectar equipos críticos. • Limitar el acceso a la Zona de Comercio Digital a quienes no cumplan con los anteriores mecanismos de seguridad acordados.
Infraestructura digital	• Garantizar la pervivencia de los espacios y entidades que representan el interés público en internet y establecer normas claras que garanticen la participación de todas las partes interesadas en la toma de decisiones. • Infraestructura de datos abierta y federada que permita acceder a les datos y compartirlos de forma segura y fiable.
Infraestructura digital	Descentralizar los servidos de almacenamiento para reducir las cuotas de mercado de los grandes jugadores.
Soberanía digital personal	• Potenciar el desarrollo y uso de nuevas arquitecturas digitales y protocolos que preserven la privacidad y devuelvan a los usuarios el control de sus datos personales. • Nuevas herramientas de monetización de contenido para creadores. • Plataformas sociales descentralizadas.
	Medidas para configurar un ecosistema de innovación digital que produzca valor para todos:

Inversión en tecnologías y ecosistemas de impacto	• Financiación de nuevas herramientas digitales en pro del bien público: redes sociales de propósito público, buscadores especializados no extractivos, nuevas tecnologías respetuosas a la hora de generar ingreses, modeles de publicidad *online* no basados en la extracción de datos íntimos, herramientas que faciliten la cocreación y la compartición solidar ia de datos, y otros servicios digitales y tecnologías cívicas. • Creación de un fondo de capital riesgo público-privado para invertir en investigaciones y en emprendimientos para la siguiente generación de plataformas con valor público. • Adoptar estructuras corporativas alternativas que permitan a las empresas compensar sus objetivos económicos con otros de corte social • Traducir a métricas operativas las misiones empresariales, los parámetros que definen la misión o razón de ser de cada organización. • Premiar los desarrollos justos. Por ejemplo, con un directorio para visibilizar y promover el uso de las herramientas digitales respetuosas que ya existen.
Medio ambiente	Extender a las grandes empresas de datos la Directiva (europea) sobre las Emisiones Industriales (DEI) para evitar o minimizar las emisiones contaminantes a la atmósfera, el agua y el suelo, con unos límites de emisión aplicables a toda la Unión Europea en relación con determinados contaminantes y con unos requisitos mínimos relativos a la inspección. Oblación de usar únicamente energías renovables para abastecer a todos sus centros de datos, sus edificios y sus campus.
Medio ambiente	• Incentivos tangibles a la innovación ecológica y de apoyo a la creación de mercados de vanguardia. • Prohibición de la obsolescencia programada. • Obligatoriedad de diseñar los dispositivos electrónicos para facilitar su reparación.
Educación, participación y servicio público	A escala nacional: • Planes específicos y ambiciosos de alfabetización digital y de capacitación tecnológica para estimular un buen uso de la tecnología y el aprovechamiento de las oportunidades que ofrece. • Sistemas de corresponsabilidad y participación organizados, transparentes, auditables, usables, efectivos y vinculantes: derecho al reconocimiento y trazabilidad de las contribuciones. • Protección efectiva de las y los «aterradores» de abusos que afectan al interés general. • Crear plataformas y redes sociales públicas, como ya se hace con otros medios de comunicación esenciales (la radio y la televisión).
Abordamiento integral	• Entender y considerar las acciones de la Alianza dentro del todo: el cuadro completo de bienestar planetario. • Evitar el «tecnosolucionismo». Poner el foco, como pilar base, en construir mejores sociedades —más inclusivas y equitativas— y mejores democracias —más participativas y transparentes—, y en educar a mejores personas y reforzar las conexiones humanas.

Apéndice 2

Relación de expertas y expertos con aportaciones destacadas en este libro

*Su inclusión no significa necesariamente que dichas fuentes apoyen todo lo que se sostiene en el libro, más allá de sus propias aportaciones.

SOLEDAD ANTELADA, ingeniera de ciberseguridad en el National Energy Research Scientific Computing Center (NERSC), del mítico Berkeley Lab (que fue parte del origen de internet). Es también directora de Seguridad de Redes de SCinet, conferencia de supercomputación de Estados Unidos que durante unos días al año se convierte en la red más potente y avanzada de la Tierra.
*Entrevistada el 26 de agosto de 2020.

MARA BALESTRINI, experta en estrategias tecnológicas e investigadora especializada en interacción humana con dispositivos. Cofundadora de la cooperativa ciudadana de datos para la investigación en salud Salus-Coop y exdirectora de la consultora de innovación de impacto Ideas for Change.
*Entrevistada el 10 de febrero de 2021.

SILVIA BARRERA, inspectora de la Policía Nacional especializada en ciberseguridad e investigación del cibercrimen. Autora de *Nuestros hijos en la red* (Barcelona, Plataforma Editorial, 2019), *Instinto y pólvora* (Barcelona, Planeta, 2018) y *Claves de la investigación en redes sociales* (Almería, Círculo Rojo, 2016).
*Entrevistada el 2 de septiembre de 2020.

ALBERT CAÑIGUERAL, especialista en economía de plataformas, conector de Ouishare para España y Latinoamérica y fundador en 2011 de ConsumoColaborativo.com. Autor de *El trabajo ya no es lo que era* (Barcelona, Conecta, 2020) y *Vivir mejor con menos* (Barcelona, Conecta, 2014).
*Entrevistado en múltiples ocasiones.

VINTON CERF, uno de los padres de internet como codiseñador de los protocolos TCP/IP y de la arquitectura de internet. Ganador, en 2004, del Premio Turing (el Premio Nobel de la informática) y de otros muchos galardones y reconocimientos. Fue vicepresidente de la Corporation for National Research Initiatives (CNRI), vicepresidente de MCI Digital Information Services, presidente de la junta directiva

de la Internet Corporation for Assigned Names and Numbers (ICANN), presidente fundador de la Internet Society (ISOC), presidente honorario del Foro IPv6 y miembro del Presidential Information Technology Advisory Committee de Estados Unidos (PITAC), entre otros muchos cargos. Desde 2005 ha ejercido como vicepresidente y *chief evangelist* de internet de Google.
*Entrevistado el 9 de abril de 2020.

ANDRÉS COLMENARES y LUCY BLACK-SWAN, fundadores del laboratorio de investigación creativa IAM (Internet Age Media) y de The One Billion Seconds Institute, una red de especialistas y comunidades en aprendizaje permanente para reinventar la economía digital e impulsar un cambio sistémico por el bien común y del planeta.
*Entrevistados el 25 de febrero de 2021.

JAVIER DE LA CUEVA, abogado, doctor en filosofía y estudioso de las relaciones entre el derecho y la tecnología. Ha defendido numerosos casos relacionados con la utilización de licencias libres de propiedad intelectual y con diferentes plataformas tecnológicas. Fue pionero de la Wikipedia española.
*Entrevistado el 25 de febrero de 2021.

JOÃO DAMAS, uno de los catorce guardianes de internet. Es investigador sénior en APNIC, uno de los cinco RIR (Regional Internet Registry) del mundo. Es miembro de la Internet Corporation for Assigned Names and Numbers (ICANN), una corporación global pública sin ánimo de lucro dedicada a mantener la seguridad, estabilidad e interoperabilidad de internet, algo que es clave en su expansión y evolución.
*Entrevistado el 24 de febrero de 2020.

DANIEL DENNETT, catedrático de filosofía y director del Center for Cognitive Studies de la Universidad Tufts. Eminente filósofo de la ciencia, conocido especialmente por su estudio sobre la conciencia, la memética y diversos aspectos de la mente y su relación con la inteligencia artificial. Es autor de múltiples libros y ha recibido numerosos reconocimientos.
*Entrevistado el 26 de junio de 2020.

JOAN DONOVAN, directora de Investigación del Shorenstein Center on Media, Politics and Public Policy, donde dirige el Technology and Social Change Project (TaSC). Lidera el campo del examen de estudios de tecnología e internet, extremismo *online*, manipulación de medios y campañas de desinformación.
*Extractos seleccionados de conversaciones con Donovan durante un taller con un grupo de académicos, periodistas, miembros de la sociedad civil y abogados en el que

participé el 22 de abril de 2019 en la Universidad de Harvard (Cambridge, Massachusetts, Estados Unidos).

BILL DUTTON, director fundador del Oxford Internet Institute (OII) y miembro del Global Cyber Security Capacity Centre (GCSCC) de la Oxford Martin School. Profesor en la School of Media and Communication de la Universidad de Leeds y profesor emérito en la Universidad del Sur de California. Fue el primer profesor de Internet Studies en la Universidad de Oxford y director nacional del Proceedings in Information and Communications Technology (PICT) del Reino Unido. Es autor de varios libros y ha recibido numerosos premios.
*Entrevistado el 6 de abril de 2019.

GEMMA GALDON CLAVELL, fundadora y directora de Eticas Research and Consulting y de Eticas Foundation. Es pionera en auditoría algorítmica ética a escala internacional y experta en ética para la Dirección General de Investigación e Innovación de la Comisión Europea. Forma parte del consejo asesor de Privacy International y Data & Ethics.
*Entrevistada en múltiples ocasiones.

ÁNGEL GÓMEZ DE ÁGREDA, coronel del Ejército del Aire y jefe del Área de Análisis Geopolítico de la División de Coordinación y Estudios de Seguridad y Defensa de la Secretaría General de Política de Defensa (SEGENPOL, Ministerio de Defensa). Ha sido jefe de cooperación del Mando Conjunto de Ciberdefensa y representante español en el Centro de Excelencia de Cooperación en Ciberseguridad de la OTAN. Es autor de *Mundo Orwell. Manual de supervivencia para un mundo hiperconectado* (Barcelona, Ariel, 2019).
*Entrevistado el 3 de marzo de 2020.

MARY L. GRAY, antropóloga e investigadora principal en Microsoft Research y presidenta de su Comité Asesor de Ética. También es profesora asociada en el Berkman Klein Center for Internet and Society de la Universidad de Harvard y miembro del Comité Permanente de la Universidad de Stanford para su proyecto AI100 sobre el futuro de la inteligencia artificial (IA). Se centra en cómo los usos cotidianos de las tecnologías por parte de las personas transforman el trabajo, la identidad y los derechos humanos. Es coautora de *Ghost Work* (Boston, Houghton Mifflin Harcourt, 2019), entre otros libros.
*Entrevistada en varias ocasiones.

ROSA GUIRADO, abogada y economista experta en regulación, competencia, mercantil, en el sector de las plataformas digitales y colaborativas, energía y otros sectores

regulados. Fundadora de Legal Sharing y consultora en estrategia jurídica de plataformas *online*.
*Entrevistada en múltiples ocasiones.

EVAN HENSHAW-PLATH, tecnólogo y primer empleado de Odeo, donde ayudó a crear Twitter. A su paso por el Center for Civic Media en el MIT Media Lab creó Affinity.works como una plataforma de promoción de código abierto. Ahora es cofundador y CEO de Planetary, una red social descentralizada. También participa en el desarrollo de Bluesky, un protocolo abierto para descentralizar las plataformas sociales.
*Entrevistado el 13 de marzo de 2021.

LORENA JAUME-PALASÍ, fundadora y directora de Ethical Tech Society. Fue cofundadora y directora de AlgorithmWatch. Experta en filosofía del derecho especializada en los aspectos éticos de la digitalización y la automatización, es miembro del Consejo Asesor de Inteligencia Artificial de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) y cofundadora de la Dynamic Coalition on Publicness del Internet Governance Forum (IGF) de las Naciones Unidas.
*Entrevistada en múltiples ocasiones.

SIMONA LEVI, cofundadora de Xnet y codirectora del curso de posgrado «Tecnopolítica y derechos en la era digital» de la Universidad de Barcelona. Forma parte del grupo asesor de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) para la creación de una Carta de Derechos Digitales.
*Entrevistada en varias ocasiones.

TIM O'REILLY, impulsor del *software* libre y de la web 2.0. Fundador y CEO de O'Reilly Media y socio de la firma de capital riesgo O'Reilly AlphaTech Ventures (OATV) y de las juntas directivas de Maker Media, Code for America, PeerJ, Civis Analytics y PopVox. Autor de varios libros, el más reciente es *La economía WTF (What The Fuck). El futuro que nos espera y por qué depende de nosotros*, trad. de Rebeca Bouvier, Barcelona, Deusto, 2018.
*Entrevistado el 28 de enero de 2020.

ROBERT RODRIGUEZ, ex agente del Servicio Secreto de Estados Unidos, en el que ejerció como agente infiltrado, responsable de la seguridad personal de los presidentes Ronald Reagan, George H.W. Bush y Bill Clinton, agente de ciberseguridad, entre otras cosas. Fundador de SINET (Security Innovation Network) y asesor del International Cyber Security Research and Development Center y del Computer Science Department de la Universidad de Stanford.

*Entrevistado el 21 de abril de 2020.

ESTHER SÁNCHEZ, abogada especialista en recursos humanos, relaciones laborales, desarrollo de la organización y liderazgo.
*Testimonio obtenido por vía telemática el 3 de diciembre de 2020.

FERNANDO SÁNCHEZ, director del Centro Nacional de Protección de Infraestructuras y Ciberseguridad de España (CNPIC) y oficial superior de la Guardia Civil.
*Entrevistado el 9 de abril de 2020.

BRUCE SCHNEIER, reconocido criptógrafo experto en ciberseguridad. Miembro del Klein Center for Internet and Society de la Universidad de Harvard, profesor de Políticas Públicas en la Harvard Kennedy School, miembro de las juntas directivas de Electronic Frontier Foundation, AccessNow y Tor Project, y asesor del Electronic Privacy Information Center (EPIC) y de VerifiedVoting.org. Es el responsable de arquitectura de seguridad de Inrupt, la nueva iniciativa de Tim Berners-Lee. Es autor de más de una docena de libros.
*Consultado por vía telemática en abril de 2020.

MARÍA SEFIDARI, presidenta de la Wikimedia Foundation, la organización matriz de Wikipedia. Fue socia fundadora y la primera vicepresidenta de Wikimedia España y cofundadora de Wikimujeres, una iniciativa centrada en reducir la brecha de género en Wikipedia. En 2014 fue nombrada *fellow* de TechWeek Women's Leadership, un programa que apoya y homenajea a mujeres líderes emergentes en empresas y tecnología. Es profesora del máster de Comunicación, Cultura y Ciudadanía Digital de la Universidad Rey Juan Carlos.
*Entrevistada el 7 de febrero de 2020.

ADAM SMITH, consultor de gestión sénior experto en servicios en la nube, ciberseguridad y soberanía digital en HiSolutions AG. Consultor y asesor de la iniciativa Gaia-X para el desarrollo de una infraestructura europea de datos en la nube.
*Entrevistado el 8 de marzo de 2021.

ANDREU VEÀ BARÓ, ingeniero de telecomunicaciones y doctor ingeniero de electrónica. Único europeo en el Consejo del Internet Hall of Fame por su «contribución significativa al desarrollo y avance de internet en todo el mundo». Conocido como «el biógrafo de internet», autor de *Cómo creamos internet* (Barcelona, Península, 2013). Premio Nacional a la Trayectoria Personal en Internet por el Senado y Premio Salvà i Campillo a la Personalidad Destacada en Telecomunicaciones e Informática, entre otros.

*Entrevistado en múltiples ocasiones.

JOHN VOELLER, ex analista de seguridad nacional en la Oficina Ejecutiva del Presidente de Estados Unidos, ex consultor del Departamento de Seguridad Nacional (DHS) de Estados Unidos y exvicepresidente de Black & Veatch, dedicada a la construcción de infraestructura humana crucial en materia de energía, agua, telecomunicaciones y servicios estatales. Ha pasado gran parte de su carrera desarrollando tecnología de automatización avanzada e inteligencia automatizada.
*Consultado por vía telemática en abril de 2020.



Esther Paniagua (Madrid, 1986) es una periodista independiente y autora especializada en ciencia y tecnología, con especial interés en el análisis del impacto social de la innovación. Publica en *El País*, *El Español (D+I)*, *Xataka y Muy Interesante*, entre otras publicaciones. Ha sido reconocida como una de las 'Top 100 Mujeres Líderes de España' en 2019 y 2020. También fue elegida entre las '100 Most Creative People in Business' por la revista *Forbes España*. Ha recibido numerosos galardones en periodismo científico, tecnológico y de innovación. Además, es profesora habitual en diversos programas de máster en temáticas relacionadas con el periodismo, la comunicación digital o la inteligencia artificial. Este es su primer libro en solitario, después *Diferencia(te)* (Edebé, 2015) del que es coautora. Vive entre Barcelona y Madrid.

Twitter: @e_paniagua
Instagram: @e_paniagua
Linkedin: estherpaniagua

[1] Toni García, «Internet se vendrá abajo y viviremos oleadas de pánico»,*El País* (2014); disponible en <https://elpais.com/cultura/2014/03/25/actualidad/1395776953_258137.xhtml>. <<

[2] Cristian Rus, «La “magia” del internet de las cosas. Caen servidores de Amazon y dejan sin funcionar a la Roomba y a timbres conectados», *Xataka* (2020); disponible en <https://www.xataka.com/otros-dispositivos/caida-parcial-servidores-amazon-ha-provocado-que-aspiradoras-dejen-funcionar>. <<

[3] Alex Hern, «Google suffers global outage with Gmail, YouTube and majority of services affected», *The Guardian* (2020); disponible en <https://www.theguardian.com/technology/2020/dec/14/google-suffers-worldwide-outage-with-gmail-youtube-and-other-services-down>. <<

[4] «French sci-fiteam called on to predict future threats», BBC (2019); disponible en <https://www.bbc.com/news/world-europe-49044892>. <<

[1] Extracto no publicado de la entrevista de Toni García con Mo Gawdat para la revista *Icon*: «Yo era un tipo que una noche se compró *online* dos Rolls-Royce porque me aburría», *El País* (2018); disponible en <https:// elpais.com/elpais/2018/ 06/04/icon/1528129934_188441.xhtml>. <<

[2] Según John Voeller, exanalista de seguridad nacional en la Oficina Ejecutiva del Presidente de Estados Unidos y exconsultor del Departamento de Seguridad Nacional (DHS) de Estados Unidos, abril de 2020. <<

[3] Entrevista a Vinton Cerf, 9 de abril de 2020. <<

[4] Entrevista a Daniel Dennett, 26 de junio de 2020. <<

[5] Toni García, «Internet se vendrá abajo y viviremos oleadas de pánico»,*El País* (2014); disponible en <https://elpais.com/cultura/2014/03/25/actualidad/1395776953_258137.xhtml>. <<

[6] «The Internet could crash. We need a Plan B. Danny Hillis», TED (2013); disponible en <https://www.ted.com/talks/danny_hillis_the_internet_could_crash_we_need_a_plan_b>. <<

[7] Entrevista a Bill Dutton, 6 de abril de 2019. <<

[8] Tal y como confiesa Soledad Antelada, ingeniera de ciberseguridad en el mítico Berkeley Lab (que fue parte del origen de internet) y directora de Seguridad de Redes de SCinet. <<

[9] Declaración de Mudge y sus compañeros de L0pht en el Senado de Estados Unidos (1998): parte I, disponible en <https://youtu.be/PQ_ F9MRpulw>; parte II, disponible en <https://youtu.be/_DN549gka7k>; parte III, disponible en <https://youtu.be/i5M7LiVZkXk>. <<

[10] Pamela Ferdin, «Into the breach»,*The Washington Post* (1998); disponible en <https://www.washingtonpost.com/archive/politics/1998/04/04/into-the-breach/8ae3cf86-fbd7-4037-a1b6-842df39d9db7/>. <<

[11] Kim Zetter, «Revealed. The Internet’s Biggest Security Hole»,*Wired* (2008); disponible en <https://www.wired.com/2008/08/revealed-the-in/>. <<

[12] Tal y como reveló Edward Snowden (Spencer Ackerman, «Snowden. NSA accidentally caused Syria's internet blackout in 2012», *The Guardian* (2014); disponible en <https://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war>). Detalles técnicos del error en Matthew Prince, «How Syria Turned Off the Internet», Cloudflare (2012); disponible en <https://blog.cloudflare.com/how-syria-turned-off-the-internet/>. <<

[13] Ibíd. <<

[14] Andrei Robachevsky, «14.000 Incidents. A 2017 Routing Security Year in Review» (2018), Internet Society; disponible en <https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/>. <<

[15] Vasileios Giotsas, «The internet is surprisingly fragile, crashes thousands of times a year, and no one is making it stronger», *The Conversation* (2019); disponible en <https://theconversation.com/the-internet-is-sur prisingly-fragile-crashes-thousands-of-times-a-year-and-no-one-is-ma king-it-stronger-120364>. <<

[16] Entrevista a João Damas, 24 de febrero de 2020. <<

[17] J. Clement, *Worldwide digital population as of April 2020*, Statista (2020); disponible en <https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=How%20many%20people%20use%20the,in%20terms%20of%20internet%20users>. <<

[18] Alvy, «Fallo generalizado de los dominios .es debido a problemas en los DNS del ESNIC», *Microsiervos* (2006); disponible en <https://www.microsiervos.com/archivo/internet/fallo-dns-es.xhtml>. <<

[19] Kieren McCarthy, «It’s begun: “First”IPv6 denial-of-service attack puts IT bods on notice Internet engineers warn this is only the beginning», *The Register* (2018); disponible en <https://www.theregister.com/2018/ 03/03/ipv6_ddos/>. <<

[20] Esha Mitra y Julia Hollingsworth, «India cuts internet around New Delhi as protesting farmers clash with police», CNN (2021); disponible en <https://edition.cnn.com/2021/02/01/asia/india-internet-cut-farmersintl-hnk/index.xhtml>. <<

[21] «Resistance to coup grows despite Myanmar’s block of Facebook», *AP* (2021); disponible en <https://apnews.com/article/myanmar-blocks-facebook-08ce7dd971655e839d6a81e7391d9e4f>. <<

[22] Pavithra Mohanlong, «How the internet shutdown in Kashmir is splintering India’s democracy», *Fast Company* (2020); disponible en <https://www.fastcompany .com/90470779/how-the-internet-shutdownin-kashmir-is-splintering-indias-democracy>. <<

[23] Jeffrey Gettleman, Vindu Goel y Maria Abi-Habib, «India Adopts the Tactic of Authoritarians. Shutting Down the Internet», *The New York Times* (2019); disponible en <https://www.nytimes.com/2019/12/17/ world/asia/india-internet-modi-protests.xhtml>. <<

[24] Se puede encontrar más información al respecto en el cap. 9, «Promesas rotas». <<

[25] Samuel Woodhams y Simon Migliano, «The Global Cost of Internet Shutdowns», Top10VPN (2021); disponible en <https://www.top 10vpn.com/cost-of-internet-shutdowns>. <<

[26] «Mobile vs. Desktop Usage in 2019», Perficient (2019); disponible en <https://www.perficient.com/insights/research-hub/mobile-vs-desktop-usage-study>. <<

[27] Bob Metcalfe, «Predicting the internet’s catastrophic collapse and ghost sites galore in 1996», *InfoWorld* (1995). <<

[28] Matt Nelson (prod.) y Stewart Sugg (dir.), *Slaughterbots*, Space Digital, Estados Unidos (2017); disponible en <https://youtu.be/9CO6M2H soIA>. <<

[29] Weizhen Tan, «“Everything you see in sci-fimovies is going to happen”, says former Google X senior executive», CNBC (2018); disponible en <https://www.cnbc.com/2018/04/18/former-google-x-seniorexecutive-mo-gawdat-on-future-tehcnology.xhtml>. <<

[1] Hisashi Hayakawa *et al*., «Long-lasting Extreme Magnetic Storm Activities in 1770 Found in Historical Documents»,*The Astrophysical Journal Letters* (2017); disponible en <https://iopscience.iop.org/article/10.3847/2041-8213/aa9661#apjlaa9661t1>. <<

[2] National Research Council of the National Academies, «Severe Space Weather Events Understanding Societal and Economic Impacts. A Workshop Report», 2008, The National Academies Press; disponible en <https://www.nap.edu/catalog/12507/severe-space-weather-events-understanding-societal-and-economic-impacts-a>. <<

[3] «Preliminary flash estimate for the fourth quarter of 2020», Eurostat (2021); disponible en <https://ec.europa.eu/eurostat/documents/portlet_file_entry/2995521/2-02022021-AP-EN.pdf/0e84de9c-0462-6868df3e-dbacaad9f49f>. <<

[4] Jason Furman y Wilson Powell III, «What the US GDP data tell us about 2020», Peterson Institute for International Economics (2021); disponible en <https://www.piie.com/blogs/realtime-economic-issues-watch/ what-us-gdp-data-tell-us-about-2020>. <<

[5] Sobre la base del PIB estadounidense de 2008 (14,71 billones de dólares), considerando la pérdida pronosticada por el informe de 2008 del National Research Council de Estados Unidos de dos billones de dólares en caso de un evento Carrington o similar. <<

[6] Erin Winick, «The space mission to buy us vital extra hours before a solar storm strikes», *MITTechnology Review* (2019); disponible en <https://www.technologyreview.com/2019/03/27/136297/the-space-mission-tobuy-us-vital-extra-hours-before-a-solar-storm-strikes/>. <<

[7] De acuerdo con Fernando Sánchez, director del Centro Nacional de Protección de Infraestructuras y Ciberseguridad de España (CNPIC). <<

[8] Lloyd’s of London, «Business Blackout», Centre for Risk Studies, Cambridge, Universidad de Cambridge, Judge Business School (2015); disponible en <https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout>. <<

[9] Anton Cherepanov y Robert Lipovsky, «Industroyer. Biggest threat to industrial control systems since Stuxnet», ESET (2017); disponible en <https://www.welivesecurity.com/2017/06/12/industroyer-biggestthreat-industrial-control-systems-since-stuxnet/>. <<

[10] Andy Greenberg, «How an Entire Nation Became Russia's Test Lab for Cyberwar», *Wired* (2017); disponible en: <https://www.wired.com/story/russian-hackers-attack-ukraine/>. <<

[11] Rebecca Smith, «Russian Hackers Reach U. S. Utility Control Rooms, Homeland Security Officials Say», *The Wall Street Journal* (2018); disponible en <https://www.wsj.com/articles/russian-hackers-reach-us-utility-control-rooms-homeland-security-officials-say-1532388110>. <<

[12] «Informe Anual de Seguridad Nacional 2019», Gobierno de España (2020); disponible en <https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2019>. <<

[13] Yuval Noah Harari, «Yuval Harari. Lecciones de un año de Covid», *La Vanguardia* (2021); disponible en <https://www.lavanguardia.com/internacional/20210314/6290059/yuval-harari-lecciones-ano-covid.amp.xhtml>. <<

[14] Vincent C. C. Cheng *et al*., «Severe Acute Respiratory Syndrome Coronavirus as an Agent of Emerging and Reemerging Infection», *Clinical Microbiology Reviews* (2007); disponible en <https://cmr.asm.org/content/20/4/660>. <<

[1] Ben Bours, «How a Dorm Room Minecraft Scam Brought Down the Internet»,*Wired* (2017); disponible en <https://www.wired.com/story/ mirai-botnet-minecraft-scam-brought-down-the-internet/>. <<

[2] Bruce Schneier, *Haz clic aquí para matarlos a todos. Un manual de supervivencia*, trad. de Álvaro Robledo, Barcelona, Temas de Hoy, 2019. <<

[3] Tal y como aseguraba Ángel Gómez de Ágreda, jefe del Área de Análisis Geopolítico de la División de Coordinación y Estudios de Seguridad y Defensa de la Secretaría General de Política de Defensa (SEGENPOL, Ministerio de Defensa) y autor de *Mundo Orwell. Manual de supervivencia para un mundo hiperconectado*, Barcelona, Ariel, 2019, durante nuestra entrevista el 3 de marzo de 2020. <<

[4] «Global Threat Report 2017», Darktrace (2017). <<

[5] Kim Zetter, *Countdown to Zero Day. Stuxnet and the Launch of the World's First Digital Weapon*, Nueva York, Broadway Books-Crown, 2014. <<

[6] Geoff White, «Love Bug’s creator tracked down to repair shop in Manila», BBC; disponible en <https://www.bbc.com/news/technology52458765>. <<

[7] Daniel Lara y Manuel V. Gómez, «El SEPE sigue paralizado por el ciberataque.“Rellenamos expedientes con formularios antiguos a mano”», *El País* (2021); disponible en <https://elpais.com/economia/2021-03-10/el-sepe-sigue-paralizado-por-el-ciberataque-rellenamos-expedientescon-formularios-antiguos-a-mano.xhtml>. <<

[8] Rafa Bernardo, «Un ataque informático paraliza al Servicio Público de Empleo», Cadena SER (2021); disponible en <https://cadenaser.com/ser/2021/03/09/economia/1615291327_568213.xhtml>. <<

[9] Según el informe «The cost of ransomware in 2021. A country-by-country analysis» de EMSISOFT; disponible en <https://blog.emsisoft.com/en/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/>. <<

[10] Las cifras oscilan según los informes. Incluimos algunas referencias: «¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?», Deloitte (2017); disponible en <https://perspectivas.deloitte.com/hubfs/Campanas /WannaCry/Deloitte-ES-informe-WannaCry.pdf>; Informe, «2017 Internet Organised Crime Threat Assessment (IOCTA)», Europol's European Cybercrime Centre (EC3); disponible en <https:// www.europol.europa.eu/iocta/2017/index.xhtml>. <<

[11] S. Ghafur *et al*., «A retrospective impact analysis of the WannaCry cyberattack on the NHS», *Nature* (2019); disponible en <https://www.nat ure.com/articles/s41746-019-0161-6>. <<

[12] Zack Whittaker, «Two years after WannaCry, a million computers remain at risk», *TechCrunch* (2019); disponible en <https://techcrunch.com/2019/05/12/wannacry-two-years-on/>. <<

[13] Rob Pegoraro, «We keep falling for phishing emails, and Google just revealed why», *Fast Company* (2019); disponible en <https://www.fastcompany.com/90387855/we-keep-falling-for-phishing-emails-and-google-just-revealed-why>. <<

[14] Informe «2019 Internet Crime Report», FBI (2020); disponible en <https://pdf.ic3.gov/2019_IC3Report.pdf>. <<

[15] «Un error en una campaña de *phishing* permite que cualquiera pueda acceder desde Google a miles de contraseñas robadas», Europa Press (2021); disponible en <https://www.europapress.es/portaltic/ciberseguridad/noticia-error-campana-phishing-permite-cualquiera-pueda-acceder-google-miles-contrasenas-robadas-20210121125710.xhtml>. <<

[16] Aaron Holmes, «Exclusive. 533 million Facebook users' phone numbers and personal data have been leaked online», *Business Insider* (2021); disponible en <https://www.businessinsider.com/stolen-data-of-533-mi llion-facebook-users-leaked-online-2021-4>. <<

[17] Raphael Satter, Christopher Bing y Joseph Menn, «Hackers used SolarWinds' dominance against it in sprawling spy campaign», Reuters (2020); disponible en <https://www.reuters.com/article/global-cyber-solarwinds-idINKBN28P2N8?edition-redirect=in>. <<

[18] «Assessing the Saudi Government’s Role in the Killing of Jamal Khashoggi», Oficina de la Directora Nacional de Inteligencia de Estados Unidos (ODNI); disponible en <https://www.dni.gov/files/ODNI/documents/assessments/Assessment-Saudi-Gov-Role-in-JK-Death-2021022 6v2.pdf>. <<

[19] Puede leerse más sobre «cibervigilancia» y «ciberespionaje» en el cap. 7. <<

[20] «Hackers Remotely Kill a Jeep on a Highway», *Wired* (2015), disponible en <https://youtu.be/MK0SrxBC1xs>. <<

[21] Índice Global de Impacto de Amenazas de Check Point, «Check Point’s Global Threat Impact Index», Check Point (agosto de 2020). <<

[22] Nicholas Kristof, «The Children of Pornhub»,*The New York Times* (2020); disponible en <https://www.nytimes.com/2020/12/04/opinion/ sunday/pornhub-rape-trafficking.xhtml>. <<

[23] Brian Heater, «Pornhub removes all unverified content, following reports of exploitation» *TechCrunch*; disponible <https://techcrunch.com/2020/12/14/pornhub-removes-all-unverified-content-following-reports-of-exploitation/>. <<

[24] Según investigaciones de la empresa de ciberseguridad Check Point hechas públicas en octubre de 2020. <<

[25] Según el estudio «Estado actual de la seguridad de los datos móviles corporativos en España» de Kingston (noviembre de 2020). <<

[26] Eugene [Yevgueni] Kaspersky, «COVID-19 has changed global cybersecurity. What must nations do now?», Kaspersky (2020); disponible en <https://www.kaspersky.com/blog/secure-futures-magazine/global-cy bersecurity-priorities/37866/>. <<

[27] Ben Collier, «Briefing Paper # 4. Boredom, routine activities, and cybercrime during the pandemic», Universidad de Cambridge, Cambridge Cybercrime Centre COVID, (2020); disponible en <https://www.cambridgecybercrime.uk/COVID/COVIDbriefing-4.pdf>. <<

[28] Silvia Barrera, inspectora de la Policía Nacional especializada en ciberseguridad e investigación del cibercrimen; autora de *Nuestros hijos en la red. 50 cosas que debemos saber para una buena prevención digital*, Barcelona, Plataforma Editorial, 2019; entrevistada el 2 de septiembre de 2020. <<

[29] Como detalla, entre otros muchos, el informe «Cybersecurity and U. S. Election Infrastructure» de *Foreign Policy* (2020); disponible en <https://foreignpolicy.com/2020/10/27/election-cybersecurity-cyberat tack-critical-infrastructure-voting>. <<

[30] James Bridle,*La nueva edad oscura. La tecnología y el fin del futuro*, trad. de Marcos Pérez Sánchez, Barcelona, Debate, 2020. <<

[1] Russell Brand, *Recovery*. *Freedom from Our Addictions*, Nueva York, Henry Holt and Co., 2017. <<

[2] Las cifras varían según los estudios. En el «Smartphone users worldwide 2016-2021» (2020), de Statista (disponible en <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide>), señalan que la penetración de los *smartphones* en España es de un 80 por ciento. La penetración asciende a un 96 por ciento en el «Estudio Anual de Mobile & Connectes Devices» (2019), elaborado por GFK y People para IAB España. La encuesta Global Mobile Consumer Survey 2017 de Deloitte realizada un año antes (disponible en <https://www2.deloitte.com/ content/dam/Deloitte/es/Documents/tecnologia-media-telecomunicacio nes/Deloitte-ES-TMT-Consumo-Movil-2017.pdf>) situaba ya la cifra en un 92 por ciento. <<

[3] «Smartphone penetration rate by country 2018», Statista (2020); disponible en <https://www.statista.com/statistics/539395/smartpho ne-penetration-worldwide-by-country>. <<

[4] «V Edición del Estudio sobre Adicción al Móvil», Rastreator (2019). <<

[5] «VI Edición del Estudio sobre Adicción al Móvil», Rastreator (2020). <<

[6] Un 66 por ciento según la encuesta «Equipamiento y uso de TIC en los hogares. Año 2019» del Instituto Nacional de Estadística (INE) (disponible en <https://ine.es/prensa/tich_2019.pdf>) y un 65 por ciento según el informe «Porcentaje de niños que tenía teléfono móvil España 2007-2019», de Statista (disponible en <https://es.statista.com/estadisticas/626309/por centaje-de-ninos-que-tenian-telefono-movil-espana/>). <<

[7] «Encuesta sobre uso de drogas en Enseñanzas Secundarias en España, ESTUDES», 2019; disponible en <https://pnsd.sanidad.gob.es/profesionales/sistemasInformacion/sistemaInformacion/pdf/ESTUDES_2018-19_Presentacion.pdf>. <<

[8] Según datos del Ministerio de Sanidad anunciados en 2018; disponible en <https://www.mscbs.gob.es/gabinete/notasPrensa.do?id=4294>. <<

[9] Laura Picazo Sánchez y Juan Carlos Ballesteros Guerra, «Las TIC y su influencia en la socialización adolescente», 2018, BBVA, Google y Fundación de Ayuda contra la Drogadicción (FAD); disponible en <https://www.observatoriodelainfancia.es/ficherosoia/documentos/5702_d_investigacion_conectados_2018.PDF>. <<

[10] Susana Méndez-Gago *et al*., «Uso y abuso de las Tecnologías de la Información y la Comunicación por adolescentes», Madrid, Universidad Camilo José Cela, 2018; disponible en <http://www.madridsalud.es/servi ciopad/wp-content/uploads/2018/06/EstudioUCJC-v3.pdf>. <<

[11] Según datos del estudio «Actitudes ante la Tecnología y Usos de las TIC en la Sociedad Española en el marco del Covid-19», Madrid, Fundación BBVA, 2021; disponible en <https://www.fbbva.es/wp-content/uploads/ 2021/02/Presentacion-Estudio-Usos-Internet-Covid19.pdf>. <<

[12] Lucija Vejmelka y Martin Mihajlov, «Internet Addiction. A Review of the First Twenty Years», *Psychiatria Danubina*, 29, 3 (2017), pp. 260-272. <<

[13] Richard Seymour, *The Twittering Machine (La máquina de trinar)*, trad. de Alcira Bixio, Madrid, Akal, 2020, <<

[14] Definidos así por la antropóloga Natasha Dow Schüll en su libro *Addiction by Design*, Princeton, Princeton University Press, 2012. <<

[15] Tim Kendall declaró el 24 de septiembre de 2020 ante el Congreso de Estados Unidos en la sesión «Hearing on mainstream extremism. Social Media's role in radicalizing America», cuyo vídeo está disponible en <https://energycommerce.house.gov/committee-activity/hearings/hea ring-on-mainstreaming-extremism-social-media-s-role-in-radicalizing>. La transcripción de su declaración está disponible en <https://docs.house.gov/meetings/IF/IF17/20200924/111041/HHRG-116-IF17-WstateKendallT-20200924.pdf>. <<

[16] Samuel P. L.Veissière y Moriah Stendel «Hypernatural Monitoring. A Social Rehearsal Account of Smartphone Addiction», *Frontiers in Psychology*, n.º 9 (2018); disponible en <https://www.frontiersin.org/articles/ 10.3389/fpsyg.2018.00141/full>. <<

[17] Ídem. <<

[18] Matthew D.Lieberman, *Social. Why Our Brains Are Wired to Connect*, Nueva York, Crown Publishers, 2013. <<

[19] John McCarthy *et al*., «The experience of enchantment in human–computer interaction», *Personal and Ubiquitous Computing*, 10,6 (2006), pp. 369-378; disponible en <https://link.springer.com/article/10.1007/ s00779-005-0055-2>. <<

[20] En su libro *Persuasive Technology. Using Computers to Change What We Think and Do*, Ámsterdam y Boston, Morgan Kaufmann Publishers, 2002, publicado cuando había ya teléfonos móviles por doquier, pero no aún *smartphones*, B. J. Fogg ya avanzaba algunas de las posibilidades de los teléfonos inteligentes. <<

[21] Russell B. Clayton *et al*., «The Extended iSelf. The Impact of iPhone Separation on Cognition, Emotion, and Physiology»,*Journal of Computer-Mediated Communication*, 20, 2 (2015), pp. 119-135; disponible en <https://academic.oup.com/jcmc/article/20/2/119/4067530>. <<

[22] Según el estudio «Y después de los Smartphone, ¿qué? Ciudadano Cyborg» (2019), elaborado por la aseguradora Línea Directa. <<

[23] Hay múltiples ejemplos. Uno reciente es «Overnight smartphone use. A new public health challenge? A novel study design based on high-resolution smartphone data», *PLOS ONE* (2018), disponible en: < https:// journals.plos.org/plosone/article?id=10.1371/journal.pone.0204811>. <<

[24] Véase nota 18. <<

[25] Estudio «Smartphones. El impacto de la adicción al móvil en los accidentes de tráfico», Fundación Línea Directa e Instituto de Tráfico y Seguridad Vial (INTRAS) de la Universitat de València, 2019; disponible en <http://revista.dgt .es/Galerias/noticia/nacional/2019/09SEPTIEMBRE/Impacto-de-la-adiccion-al-movil -en-los-accidentes-de-trafico_DEF.pdf>. <<

[26] «Digital Distraction in the Workplace», EMI Research Solutions y Stark Statistical Consulting, *Screen Education* (2019); disponible en <https://www.screeneducation.org/digital-distraction-in-the-workplace.html>. <<

[27] Según un experimento realizado por las universidades de Wurzburgo (Alemania) y Nottingham Trent (Reino Unido) para Kaspersky Lab en 2016. <<

[28] Adrian F. Ward *et al.*, «Brain Drain. The Mere Presence of One's Own Smartphone Reduces Available Cognitive Capacity», *Journal of the Association for Consumer Research* (2017), University of Chicago Press; disponible en: <https://www.journals.uchicago.edu/doi/abs/10.1086/691462>. <<

[29] Bernard McCoy, «Digital Distractions in the Classroom. Student Classroom Use of Digital Devices for Non-Class Related Purposes» (2013), Universidad de Nebraska-Lincoln; disponible en <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1070&context=journalismfacpub>. <<

[30] Richard E. Mayer y Roxana Moreno, «Nine Ways to Reduce Cognitive Load in Multimedia Learning», *Educational Psychologist* (2003); disponible en <https://www.tandfonline.com/doi/abs/10.1207/S15326985 EP3801_6>. <<

[31] Jeffrey H. Kuznekoff y Scott Titsworth, «The Impact of Mobile Phone Usage on Student Learning», *Communication Education* (2013); disponible en <https://www.tandfonline.com/action/showCitFormats?doi=10.1080%2F03634523.2013.767917>; Larry D. Rosen *et al*., «Un estudio empírico del efecto de los cambios de tarea en el aula inducidos por los mensajes de texto. Implicaciones para la enseñanza y estrategias para la mejora del aprendizaje», *Psicología Educativa* (2011), Colegio Oficial de Psicólogos de Madrid; disponible en <https://doi.org/10.5093/ed2011v17 n2a4>. <<

[32] Sana Faria *et al*., «Laptop multitasking hinders classroom learning for both users and nearby peers», *Computers & Education* (2011); disponible en <https://www.sciencedirect.com/science/article/pii/S036013151200 2254?via%3Dihub>. <<

[33] Deborah R. Tindell y Robert W. Bohlander, «The Use and Abuse of Cell Phones and Text Messaging in the Classroom. A Survey of College Students», *College Teaching* (2012); disponible en <https://www.tandfonline.com/doi/abs/10.1080/87567555.2011.604802>. <<

[34] Encuesta a cuatrocientas familias españolas con hijos de entre dos y ocho años realizada por la plataforma de aprendizaje de inglés Lingokids en 2019. <<

[35] Michel Desmurget, *La fábrica de cretinos digitales. Los peligros de las pantallas para nuestros hijos*, trad. de Lara Cortés, Barcelona, Península, 2020. <<

[36] Ídem. <<

[37] Véase nota 9. <<

[38] «Qustodio 2020 annual report on children's digital habits», Qustodio (2020); disponible en <https://qweb.cdn.prismic.io/qweb/f5057b933d28-4fd2-be2e-d040b897f82d_ADR_en_Qustodio+2020+report.pdf>. <<

[39] Sarah Marsh, «TikTok investigating videos promoting starvation and anorexia», *The Guardian* (2020); disponible en <https://www.theguardian.com/technology/2020/dec/07/tiktok-investigating-videos-promoting-starvation-and-anorexia>. <<

[40] Ídem. <<

[41] Matt Richtel, «Children’s Screen Time Has Soared in the Pandemic, Alarming Parents and Researchers», *The New York Times* (2021); dispo-nible en <https://www.nytimes.com/2021/01/16/health/covid-kids-tech-use.xhtml>. <<

[42] Como hemos visto en el cap. 3. <<

[43] Tal y como comenta Silvia Barrera, inspectora de la Policía Nacional especializada en ciberseguridad e investigación del cibercrimen y autora de *Nuestros hijos en la red. 50 cosas que debemos saber para una buena prevención digital*, Barcelona, Plataforma Editorial, 2019. Entrevista realizada el 2 de septiembre de 2020. <<

[44] Esther Paniagua, «Así triunfa una red social sin seguidores,“likes” ni comentarios», *Retina*, *El País* (2019); disponible en <https://retina.elpais.com/retina/2020/01/03/tendencias/1578056349_169377.xhtml>. <<

[45] Cecilie Schou Andreassen, «Online Social Network Site Addiction. A Comprehensive Review», *Current Addiction Reports* (2015); disponible en <https://link.springer.com/article/10.1007%2Fs40429-015-0056-9>. <<

[46] Según el informe «Young people’s mental and emotional health», del Education Policy Institute y The Prince’s Trust del Reino Unido, disponible en <https://epi.org.uk/wp-content/uploads/2021/01/EPI-PT_ Young-people%E2%80%99s-wellbeing_Jan2021.pdf>. <<

[47] Gadi Lissak, «Adverse physiological and psychological effects of screen time on children and adolescents. Literature review and case study», *Environmental Research* (2018); disponible en <https://www.sciencedirect.com/science/article/abs/pii/S001393511830015X?via%3Dihub>. <<

[48] Tanya Basu, «Facebook just invented Facebook», *MIT Technology Review* (2020); disponible en <https://www.technologyreview.com/2020/09/10/1008269/facebook-just-invented-facebook-campus/>. <<

[49] Sergio C. Fanjul, «El bar de copas ya estaba moribundo antes del coronavirus. Así llegó la crisis de un símbolo de la noche española», *Icon*, *El País* (2020); disponible en <https://elpais.com/elpais/2020/09/16/icon/1600249587_369373.xhtml>. <<

[50] Canela López , «6 tech executives who raise their kids tech-free or seriously limit their screen time», *Business Insider* (2020), disponible en <https://www.businessinsider.com/tech-execs-screen-time-children-billgates-steve-jobs-2019-9?IR=T>; Jenny McCartney, «Tech gurus don’t let their kids have smartphones. Here’s why», *The Spectator Australia* (2018); disponible en <https://www.spectator.com.au/2018/09/tech-gurus-dontlet-their-kids-have-smartphones-heres-why/>; Nick Bilton, «Steve Jobs Was a Low-Tech Parent», *The New York Times* (2014); disponible en <https://www.nytimes.com/2014/09/11/fashion/steve-jobs-apple-was-alow-tech-parent.xhtml>. <<

[51] Véase <https://www.humanetech.com/>. Al principio se llamó Time Well Spent o «tiempo bien empleado». <<

[1] Del Gobierno de Thomas Woodrow Wilson, presidente de Estados Unidos entre 1913 y 1921. <<

[2] *Cristalizando la opinión pública*, trad. de Ernesto Gómez Cereijo, Barcelona, Gestión 2000, 1998. <<

[3] Edward L. Bernays, «The Engineering of Consent»,*The Annals of the American Academy of Political and Social Science* (1947); disponible en <https://journals.sagepub.com/doi/10.1177/000271624725000116>. <<

[4] *Propaganda*, trad. de Albert Fuentes Sánchez, Barcelona, Melusina, 2008. <<

[5] Definición de la Comisión Europea para el concepto de «desinformación». <<

[6] En palabras de Joan Donovan, directora de investigación del Shorenstein Center on Media, Politics and Public Policy de la Harvard Kennedy School y responsable del Technology and Social Change Project (TaSC), durante un taller con un grupo de estudiosos, periodistas, miembros de la sociedad civil y abogados en el que participé el 22 de abril de 2019 en la Universidad de Harvard (en Cambridge, Massachusetts, Estados Unidos). <<

[7] Vic Zoschak, «A Brief History of Propaganda», The International League of Antiquarian Booksellers (ILAB) (2014); disponible en <https:// ilab.org/articles/brief-history-propaganda>. <<

[8] Tal y como explica la egiptóloga JacquelynWilliamson en «Cleopatra and Fake News. How ancient Roman political needs created a mythic temptress», Folger Shakespeare Library, *Shakespeare & Beyond* (2017); disponible en <https://shakespeareandbeyond.folger.edu/2017/10/20/cleopa tra-mythic-temptress/?_ga=2.45348769.481991007.1602245654-106692 4633.1602245654>. <<

[9] Con permiso de G. A. Bécquer, parafraseando su célebre poema: «¿Qué es poesía?, dices mientras clavas / en mi pupila tu pupila azul. / ¡Qué es poesía! ¿Y tú me lo preguntas? / Poesía eres tú», *Rimas*, rima XXI, Madrid, Castalia, 1974, p. 122. <<

[10] Definición de «trolear» de FundéuRAE; disponible en <https://www.fundeu.es/recomendacion/trolear-troleo/>. <<

[11] Justin Cheng *et al*., «Anyone Can Become a Troll. Causes of Trolling Behavior in Online Discussions», Conference on Computer-Supported Cooperative Work (CSCW) (2017); disponible en <https://files.clr3.com/papers/2017_anyone.pdf>. <<

[12] Según el informe «Bad Bot Report 2020» de Imperva. <<

[13] Florian Gallwitz y Michael Kreil, «The Rise and Fall of “Social Bot” Research» (2021); disponible en <https://papers.ssrn.com/sol3/pa pers.cfm? abstract_id=3814191>. <<

[14] Marc J.Dupuis y Andrew Williams,«The Spread of Disinformation on the Web. An Examination of Memes on Social Networking», IEEE, 2019; disponible en <https://ieeexplore.ieee.org/document/9060100>. <<

[15] Claire Wardle, «Misinformation Has Created a New World Disorder», *Scientific American* (2019); disponible en <https://www.scientificamerican.com/article/misinformation-has-created-a-new-world-disorder/>. <<

[16] Como se explica en el cap. 4. <<

[17] Titulares correspondientes a algunos de los bulos desmentidos por Maldita <www.maldita.es>, iniciativa española de monitoreo y verificación de contenido; disponible en <https://maldita.es/tag/coronavi rus+bulos/>. <<

[18] En el mes previo al decreto de estado de alarma hubo un 32,5 por ciento de bulos, que aumentó a un 67,5 por ciento en el mes posterior, según el estudio «Infodemia y COVID-19. Evolución y viralización de informaciones falsas en España», de José Manuel Sánchez-Duarte y Raúl Magallón Rosa, *Revista Española de Comunicación en Salud* (2020); disponible en <https://doi.org/10.20318/recs.2020.5417>. <<

[19] Según me comentó Kathleen Carley —directora del Center for Informed Democracy and Social-cybersecurity (IDeaS) y del Center for Computational Analysis of Social and Organizational Systems (CASOS)— durante un debate *online* organizado por el centro de diplomacia científica y tecnológica de Barcelona SciTech DiploHub el 11 de mayo de 2020. <<

[20] Catherine Stupp, «Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case», *The Wall Street Journal* (2019); disponible en <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voicein-unusual-cybercrime-case-11567157402>. <<

[21] Karen Hao, «A deepfake bot is being used to “undress” underage girls», *MIT Technology Review* (2020); disponible en <https://www.technologyreview.com/2020/10/20/1010789/ai-deepfake-bot-undresses-women-and-underage-girls/>. <<

[22] Rana Ayyub, «I Was The Victim Of A Deepfake Porn Plot Intended To Silence Me», *Huffington Post* (2018); disponible en <https://www.huffington post.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316>. <<

[23] Samantha Cole, Emanuel Maiberg y Anna Koslerova, «“Frankenstein’s Monster”. Images of Sexual Abuse Are Fueling Algorithmic Porn», *Vice* (2020); disponible en <https://www.vice.com/en/article/akdgnp/ sexual-abuse-fueling-ai-porn-deepfake-czech-casting-girls-do-porn>. <<

[24] Rob Toews, «Deepfakes Are Going To Wreak Havoc On Society. We Are Not Prepared», *Forbes* (2020); disponible en <https://www.forbes.com/sites/robtoews/2020/05/25/deepfakes-are-going-to-wreak-havocon-society-we-are-not-prepared/>. <<

[25] «Journalism,“Fake news” & Disinformation», Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco) (2018); disponible en <https://en.unesco.org/sites/default/files/journa
lism_fake_news_disinformation_print_friendly_0.pdf>. <<

[26] Tim Kendall declaró el 24 de septiembre de 2020 ante el Congreso de Estados Unidos en la sesión «Hearing on mainstream extremism. Social Media's role in radicalizing America», cuyo vídeo está disponible en <https://energycommerce.house.gov/committee-activity/hearings/hearing-on-mainstreaming-extremism-social-media-s-role-in-radicalizing>. La transcripción de su declaración está disponible en <https://docs.house.gov/meetings/IF/IF17/20200924/111041/HHRG-116-IF17-WstateKendallT-20200924.pdf>. <<

[27] Definición extraída del micrositio web «Infodemic» de la OMS; disponible en <https://www.who.int/health-topics/infodemic#tab=tab_1>. <<

[28] Como recoge la FundéuRAE <https://www.fundeu.es/recomendacion/infodemia/>. <<

[29] Sune Lehmann *et al*., «Accelerating dynamics of collective attention», *Nature Communications* (2019); disponible en <https://www. nature.com/articles/s41467-019-09311-w>. <<

[30] «*Granja de clics*, mejor que *click farm*», 2019, FundéuRAE; disponible en <https://www.fundeu.es/recomendacion/granja-de-clics-mejor-queclick-farm/>. <<

[31] Peter Pomerantsev, *This Is Not Propaganda. Adventures in the War Against Reality*, Nueva York, Public Affairs, 2019. <<

[32] Ben Nimmo, «Measuring Traffic Manipulation on Twitter», Oxford Internet Institute (2019); disponible en <https://comprop.oii.ox.ac.uk/wpcontent/uploads/sites/93/2019/01/Manipulating-Twitter-Traffic.pdf>. <<

[33] *Yo, jefe del servicio secreto militar soviético*, trad. de M. B., pról., y notas de Mauricio Carlavilla, Barcelona, Radar, s. f. <<

[34] Como argumenta P. Pomerantsev en su libro *This Is Not Propaganda…* <<

[35] Definida así por el *Oxford English Dictionary*, que en 2016 seleccionó «posverdad» como palabra del año: <https://languages.oup.com/ word-of-the-year/2016/>. <<

[36] Eli Pariser, *El filtro burbuja. Cómo la red decide lo que leemos y lo que pensamos*, trad. de Mercedes Vaquero, Madrid, Taurus, 2017. <<

[37] Richard Fletcher, «The truth behind filter bubbles. Bursting some myths», Reuters Institute-University of Oxford (2020); disponible en <https://reutersinstitute.politics.ox.ac.uk/risj-review/truth-behind-filterbubbles-bursting-some-myths>. <<

[38] El concepto lo acuñó el historiador social de la ciencia Iain Boal en 1992 y lo popularizaron más tarde los profesores de la Universidad de Stanford Robert Proctor y Londa Schiebinger en su libro *Agnotology. The Making and Unmaking of Ignorance*, Stanford (California), Stanford University Press, 2008. <<

[39] Danah Boyd, «The Fragmentation of Truth», Knight Media Forum (2019); disponible en <https://vimeo.com/319934136>. <<

[40] Así seguía siendo en junio de 2021, y al menos desde marzo de 2019. <<

[41] Lo dice David Prager, cofundador de PragerU, en un vídeo cuyo enlace no compartiré por motivos de responsabilidad periodística (fomentar el clic en este contenido contribuiría a la darle mayor visibilidad). <<

[42] Como explica Kevin Roose en su artículo «What Is QAnon, the Viral Pro-Trump Conspiracy Theory?», *The New York Times* (2020); disponible en <https://www.nytimes.com/article/what-is-qanon.xhtml>. <<

[43] Jessica Guynn, «Trump believes QAnon claim it’s fighting pedophiles, refuses to disavow extremist conspiracy theory», *Usa Today* (2020); disponible en <https://eu.usatoday.com/story/tech/2020/10/15/ trump-believes-qanon-claim-fighting-pedophiles/3673377001>. <<

[44] Peter Baker y Sabrina Tavernise, «One Legacy of Impeachment. The Most Complete Account So Far of Jan. 6», *The New York Times* (2021), disponible en <https://www.nytimes.com/2021/02/13/us/politics/ capitol-riots-impeachment-trial.xhtml>. <<

[45] Clare Hymes, Cassidy McDonald y Eleanor Watson, «What we know about the “unprecedented” U. S. Capitol riot arrests», CBS News (2021); disponible en <https://www.cbsnews.com/news/capitol-riotarrests-2021-05-07/>. <<

[46] Véase nota 43. <<

[47] Ídem. <<

[48] Ídem. <<

[49] «In Myanmar, Facebook struggles with a deluge of disinformation», *The Economist* (2020); disponible en <https://www.economist.com/ asia/2020/10/22/in-myanmar-facebook-struggles-with-a-deluge-ofdisinformation>. <<

[50] Ídem. <<

[51] La proporción de ingresos que se destinó al 1 por ciento más rico de la población mundial aumentó en cuarenta y seis de los cincuenta y siete países y áreas con datos de 1990 a 2015. El 40 por ciento menos rico ganó menos del 25 por ciento de los ingresos en los noventa y dos países con datos. Si bien la desigualdad entre países está disminuyendo en términos relativos, esto se debe en gran medida al fuerte crecimiento económico de China y de otras economías emergentes de Asia, una convergencia que no se distribuye de manera uniforme y que hace que las diferencias entre algunos países y áreas sigan siendo considerables, según el informe «World Social Report 2020. Inequality in a rapidly changing world», de la Organización de las Naciones Unidas (ONU); disponible en <https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2020/01/World-Social-Report-2020-FullReport.pdf>. <<

[52] Según aseguran expertos de la ONU. Fuente: «El mundo de hoy es más rico, pero también más desigual que nunca», ONU, 2018; disponible en <https://news.un.org/es/story/2018/12/1447091>. <<

[1] Julia Carrie Wong, «The viral selfie app ImageNet Roulette seemed fun until it called me a racist slur», *The Guardian* (2019); disponible en <https://www.theguardian.com/technology/2019/sep/17/imagenetroulette-asian-racist-slur-selfie?CMP=Share_iOSApp_Other>. <<

[2] Lo cuenta en un hilo en Twitter, disponible en <https://twitter.com/stephenkb/status/1173566714543595520?s=20>. <<

[3] Calificada así por Kate Crawford, cofundadora del Instituto AI Now en la Universidad de Nueva York. <<

[4] Es la conclusión del sonado artículo científico «Semantics derived automatically from language corpora contain human-like biases» (Aylin Caliskan *et al*., *Science* (2017); disponible en <https://science.sciencemag.org/ content/356/6334/183.full>) y de muchos otros publicados desde entonces. <<

[5] Cathy O’Neil, *Armas de destrucción matemática. Cómo el big data aumenta la desigualdad y amenaza la democracia*, trad. de Violeta Arranz de la Torre, Madrid, Capitán Swing, 2018. <<

[6] Algorithmic Decision Making. <<

[7] Oscar Schwartz, «Untold History of AI. Algorithmic Bias Was Born in the 1980s», *IEEE Spectrum* (2019); disponible en <https://spectrum.ieee.org/tech-talk/tech-history/dawn-of-electronics/untold-history-of-ai-thebirth-of-machine-bias>. <<

[8] Virginia Eubanks, *La automatización de la desigualdad. Herramientas de tecnología avanzada para supervisar y castigar a los pobres*, trad. de Gemma Deza, Madrid, Capitán Swing, 2021. <<

[9] Julia Angwin *et al.*, «Machine Bias. There’s software used across the country to predict future criminals. And it’s biased against blacks»,*ProPublica* (2016); disponible en <https://www.propublica.org/article/machine-biasrisk-assessments-in-criminal-sentencing>. <<

[10] En opinión de Christopher Markou, profesor e investigador especializado en leyes e inteligencia artificial de la Universidad de Cambridge (Reino Unido). Entrevista realizada el 16 de abril de 2019. <<

[11] Julia Angwin *et al*., «Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk», *ProPublica* (2017); disponible en <https://www.propublica.org/article/minorityneighborhoods-higher-car-insurance-premiums-white-areas-same-risk>. <<

[12] Julia Angwin *et al*., «When Algorithms Decide What You Pay», *ProPublica* (2017); disponible en <https://www.propublica.org/article/ breaking-the-black-box-when-algorithms-decide-what-you-pay>. <<

[13] Julia Angwin *et al*., «Facebook Lets Advertisers Exclude Users by Race», *ProPublica* (2016); disponible en <https://www.propublica.org/ article/facebook-lets-advertisers-exclude-users-by-race>. <<

[14] Julia Angwin *et al*., «Facebook Ads Can Still Discriminate Against Women and Older Workers, Despite a Civil Rights Settlement», *ProPublica* (2019); disponible en <https://www.propublica.org/article/facebook-adscan-still-discriminate-against-women-and-older-workers-despite-a-civilrights-settlement>. <<

[15] Piotr Sapiezynski *et al*., «Algorithms that “Don’t See Color”. Comparing Biases in Lookalike and Special Ad Audiences», *arXiv* (2019); disponible en <https://arxiv.org/pdf/1912.07579.pdf>. <<

[16] Testimonio de Esther Sánchez, obtenido mediante conversación telemática en diciembre de 2020. <<

[17] Como ella misma relata en Alex Lee, «An AI to stop hiring bias could be bad news for disabled people», *Wired* (2019); disponible en <https://www.wired.co.uk/article/ai-hiring-bias-disabled-people>. <<

[18] Como explica C. O’Neil (véase nota 5). <<

[19] Patente de Facebook de 2015: «Authorization and authentication based on an individual’s social network»; disponible en <http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=9100400.PN.&OS=PN/9100400&RS=PN/9100400>. <<

[20] Como reveló Colin Lecher en «What happens when an algorithm cuts your health care», *The Verge* (2016); disponible en <https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithmarkansas-cerebral-palsy>. <<

[21] Ziad Obermeyer *et al*., «Dissecting racial bias in an algorithm used to manage the health of populations»,*Science* (2019); disponible en <https://science.sciencemag.org/content/366/6464/447>. <<

[22] Natasha Singer, «Where Do Vaccine Doses Go, and Who Gets Them? The Algorithms Decide», *The New York Times* (2021); disponible en <https://www.nytimes.com/2021/02/07/technology/vaccine-algorithms.xhtml>. <<

[23] Matt Burgess, «Police built an AI to predict violent crime. It was seriously flawed», *Wired* (2020); disponible en <https://www.wired.co.uk/ article/police-violence-prediction-ndas>. <<

[24] «Home Office drops “racist” algorithm from visa decisions», BBC (2020); disponible en <https://www.bbc.com/news/technology- 53650758>. <<

[25] Jessica Murray, «Student who wrote story about biased algorithm has results downgraded»,*The Guardian* (2020); disponible en <https://www.theguardian.com/education/2020/aug/18/ashton-a-level-studentpredicted-results-fiasco-in-prize-winning-story-jessica-johnson-ashton>. <<

[26] Como señala Lorena Jaume-Palasí, fundadora de Ethical Tech Society, entrevistada en varias ocasiones. <<

[27] Según informa la nota de prensa de la Policía Nacional en la web del Ministerio del Interior; disponible en <www.interior.gob.es/prensa/ noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/9496864>. <<

[28] Tal y como recoge Karma Peiró en el apartado dedicado a España del informe «Automating Society Taking Stock of Automated DecisionMaking in the EU», *AlgorithmWatch* y Bertelsmann Stiftung (2019); disponible en <https://algorithmwatch.org/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf>. <<

[29] Ídem. <<

[30] Jim Waterson, «Microsoft sacks journalists to replace them with robots», *The Guardian* (2020); disponible en <https://www.theguardian.com/technology/2020/may/30/microsoft-sacks-journalists-to-replacethem-with-robots>. <<

[31] JimWaterson, «Microsoft’s robot editor confuses mixed-race Little Mix singers», *The Guardian* (2020); disponible en <https://www.theguardian.com/technology/2020/jun/09/microsofts-robot-journalist-confusedby-mixed-race-little-mix-singers>. <<

[32] Nicolas Kayser-Bril, «Female historians and male nurses do not exist, Google Translate tells its European users», AlgorithmWatch (2020); disponible en <https://algorithmwatch.org/en/google-translate-genderbias/>. <<

[33] Esther Paniagua, «Los asistentes de voz no deberían tener género», *Retina*, *El País* (2020); disponible en <https://elpais.com/retina/2020/01/27/innovacion/1580114979_118922.xhtml>. <<

[34] Ídem. <<

[35] Experimento realizado por Nicolas Kayser-Bril, de AlgorithmWatch, cuyos resultados publicó en «Spam filters are efficient and uncontroversial. Until you look at them», AlgorithmWatch (2020); disponible en <https://algorithmwatch.org/en/story/spam-filters-outlook-spamassassin/>. <<

[36] Para descubrir más casos de algoritmos con impacto social recomiendo el buscador del observatorio OASI (Observatory of Algorithms with Social Impact) de Eticas Foundation: <https://eticasfoundation.org/ algorithms/>. <<

[37] Daniel Dennet, «De las bacterias a Bach. La evolución de la mente», *Pasado & Presente* (2017). <<

[38] Para más información, véase Mark Harris, «NTSB Investigation Into Deadly Uber Self-Driving Car Crash Reveals Lax Attitude Toward Safety», *IEEE Spectrum* (2019); disponible en <https://spectrum.ieee.org/ cars-that-think/transportation/self-driving/ntsb-investigation-into-deadlyuber-selfdriving-car-crash-reveals-lax-attitude-toward-safety>. <<

[39] Como comenta Gemma Galdon Clavell, experta en protección de datos, fundadora de Eticas Research & Consulting y Eticas Foundation, entrevistada en múltiples ocasiones. <<

[40] Ruha Benjamin, *Race After Technology. Abolitionist Tools for the New Jim Code*, Cambridge (Reino Unido), Polity Press, 2019. <<

[41] Ídem. <<

[42] Véase nota 8. <<

[43] Concepto acuñado, en 2019, por Shoshana Zuboff en *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder*, trad. de Albino Santos, Barcelona, Paidós, 2020. <<

[1] Jeremy Bentham, *Panopticon Letters*, 1791, disponible en <http:// transcribe-bentham.ucl.ac.uk/td/JB/550/207/001>. <<

[2] Ángel Gómez Fuentes, «Condenan a una madre por subir fotos de su hijo a Facebook», *ABC* (2018); disponible en <https://www.abc.es/ sociedad/abci-condenan-madre-subir-fotos-hijo-facebook-20180118 1003_noticia.xhtml>. <<

[3] Según una demanda presentada en Europa por el navegador web privado Brave, la organización Open Rights Group y el University College de Londres, que acusan al buscador de violación del Reglamento General de Protección de Datos (RGPD) por «fuga masiva de datos muy íntimos». <<

[4] Esther Paniagua, «Así subasta Google tus datos *online*», *Retina*, *El País* (2019); disponible en <https://retina.elpais.com/retina/2019/05/28/tendencias/1559040361_176907.xhtml>. <<

[5] Geoffrey A. Fowler, «It’s the middle of the night. Do you know who your iPhone is talking to?», *The Washington Post* (2019); disponible en <https://www.washingtonpost.com/technology/2019/05/28/its-middlenight-do-you-know-who-your-iphone-is-talking/>. <<

[6] Según me explicaba Pilar Vila, perita informática y analista forense digital para el artículo «¿Tú también, Apple? Así se filtran los datos de tu iPhone» publicado en *Retina*, *El País* (2019); disponible en <https://retina.elpais.com/retina/2019/06/06/innovacion/1559816217_561514.xhtml>. <<

[7] Zack Whittaker, «Many popular iPhone apps secretly record your screen without asking», *TechCrunch* (2019); disponible en <https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots>. <<

[8] Según la «demanda bajo el artículo 22.2 de la ley 34/2002» presentada por Noyb en colaboración con Xnet ante la Agencia Española de Protección de Datos el 16 de noviembre de 2020; disponible en <https://noyb.eu/sites/ default/files/2020-11/IDFA_ES_DEF_Redacted.pdf?mtc=j>. <<

[9] Ídem. <<

[10] Tal y como pudo comprobar la periodista Kari Paul: «“They know us better than we know ourselves”. How Amazon tracked my last two years of reading»,*The Guardian* (2020); disponible en <https://www.theguardian.com/technology/2020/feb/03/amazon-kindle-data-reading-trackingprivacy>. <<

[11] Julien Gamba *et al*., «An Analysis of Pre-installed Android Software», 41th IEEE Symposium on Security and Privacy, IEEE, 2020; disponible en <https://ieeexplore.ieee.org/abstract/document/9152633>. <<

[12] «How Apps on Android Share Data with Facebook (even if you don’t have a Facebook account)», Privacy International (2018); disponible en <https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf>. <<

[13] Roger McNamee, «I Mentored Mark Zuckerberg. I Loved Facebook. But I Can’t Stay Silent About What’s Happening»,*Time Magazine* (2019); disponible en <https://time.com/magazine/us/5505429/january28th-2019-vol-193-no-3-u-s/>. <<

[14] Entrevista realizada el 26 de julio de 2017 y publicada en la revista *Papel* de *El Mundo*; disponible en <https://www.elmundo.es/papel/lideres/2017/09/12/59b7bff2e2704e25488b45f7.xhtml>. <<

[15] Edward Snowden,*Permanent Record*, Nueva York, Macmillan, 2019. [Hay trad. cast.: *Vigilancia permanente*, trad. de Esther Cruz Santaella, Barcelona, Planeta, 2020.] <<

[16] Ídem. <<

[17] Ídem. <<

[18] «Metadata. Piecing Together a Privacy Solution» (2014), American Civil Liberties Union (ACLU) de California; disponible en <https://www.aclunc.org/sites/default/files/Metadata%20report%20FINAL%202%2021%2014%20cover%20%2B%20inside%20for%20web%20%283%29.pdf>. <<

[19] John Battelle, «The Database of Intentions», *John Battelle's Search Blog* (2003); disponible en <https://battellemedia.com/archives/2003/11/the_database_of_intentions>. <<

[20] David Cole, «We Kill People Based on Metadata», *The New York Review* (2014); disponible en <https://www.nybooks.com/daily/2014 /05/10/we-kill-people-based-metadata/>. <<

[21] Lars Backstrom y Jon Kleinberg, «Romantic partnerships and the dispersion of social ties», *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, *CSCW '14*, Association for Computing Machinery (2014); disponible en <https://dl.acm.org/doi/abs/10.1145/2531602.2531642>. <<

[22] Erheng Zhonga *et al*., «User demographics prediction based on mobile data»,*Pervasive and Mobile Computing* (2013); disponible en <https://www.sciencedirect.com/science/article/abs/pii/S1574119213000916#!>. <<

[23] Jonathan Mayer *et al.*, «Evaluating the privacy properties of telephone metadata»,*PNAS* (2016); disponible en <https://www.pnas.org/content/113/20/5536#ref-38>. <<

[24] Por este motivo, la Comisión Europea está investigando la adquisición de Fitbit por parte de Google. «Mergers. Commission opens in-depth investigation into the proposed acquisition of Fitbit by Google», Comisión Europea; disponible en <https://ec.europa.eu/commission/ presscorner/detail/en/ip_20_1446>. <<

[25] «Google, Amazon Patent Filings Reveal Digital Home Assistant Privacy Problems»,*Consumer Watchdog* (2017); disponible en <https://www.consumerwatchdog.org/sites/default/files/2017-12/Digital%20Assistants%20and%20Privacy.pdf>. <<

[26] Ídem. <<

[27] Ídem. <<

[28] Ídem. <<

[29] Medios de todo el planeta se hicieron eco de la noticia, publicada originalmente por el canal de televisión local KIRO-TV. Véase Gary Horcher, «Woman says her Amazon device recorded private conversation, sent it out to random contact», KIRO 7 News (2018); disponible en <https://www.kiro7.com/news/local/woman-says-her-amazon-device-recorded-privateconversation-sent-it-out-to-random-contact/755507974/>. <<

[30] Rachel Metz, «Yes, Alexa is recording mundane details of your life, and it’s creepy as hell», *MIT Technology Review* (2018); disponible en <https://www.technologyreview.com/2018/05/25/142713/yes-alexa-is-recordingmundane-details-of-your-life-and-its-creepy-as-hell/>. <<

[31] Matt Day *et al*., «Amazon Workers Are Listening to What You Tell Alexa. A global team reviews audio clips in an effort to help the voiceactivated assistant respond to commands», Bloomberg (2019); disponible en <https://www.bloomberg.com/news/articles/2019-04-10/is-anyonelistening-to-you-on-alexa-a-global-team-reviews-audio>. <<

[32] Jamie Tarabay y Kartikay Mehrotra, «Clubhouse Chats Are Breached, Raising Concerns Over Security», Bloomberg (2021); disponible en <https://www.bloomberg.com/news/articles/2021-02-22/clubhousechats-are-breached-raising-concerns-over-security>. <<

[33] Jack Cable *et al*.,«Clubhouse in China. Is the data safe?», Stanford Internet Observatory (2021); disponible en <https://cyber.fsi.stanford.edu/ io/news/clubhouse-china>. <<

[34] «The Facial RecognitionWorld Map», Surfshark (2020); disponible en <https://surfshark.com/facial-recognition-map>. <<

[35] Ídem. <<

[36] Según el informe «Artificial Intelligence Index Report 2019» de la Universidad de Stanford; disponible en <https://hai.stanford.edu/sites/default/files/ai_index_2019_report.pdf>. <<

[37] Isabel Rubio, «Las claves de la polémica por el uso de reconocimiento facial en los supermercados de Mercadona», *El País* (2020); disponible en <https://elpais.com/tecnologia/2020-07-06/las-claves-de-lapolemica-por-el-uso-de-reconocimiento-facial-en-los-supermercados-demercadona.xhtml>. <<

[38] Kashmir Hill, «The Secretive Company That Might End Privacy as We Know It», *The New York Times* (2020); disponible en: <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recog nition.xhtml>. <<

[39] Caroline Haskins *et al*., «Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart and The NBA», *BuzzFeed* (2020); disponible en <https://www.buzzfeednews.com/ article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>. <<

[40] Como denuncia la American Civil Liberty Union de Michigan en «ACLU of Michigan complaint re use of facial recognition»: disponible en <https://www.aclu.org/letter/aclu-michigan-complaint-re-use-facialrecognition>. <<

[41] Thomas Brewster, «London Police Facial Recognition “Fails 80% Of TheTime And Must Stop Now”»,*Forbes* (2019); disponible en <https://www.forbes.com/sites/thomasbrewster/2019/07/04/london-police-facialrecognition-fails-80-of-the-time-and-must-stop-now/>; Pete Fussey y Daragh Murray, «Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology», Universidad de Essex, 2019; disponible en <https://48ba3m4eh2bf2ksp43rq8kkwpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-MetPolice-Trial-of-Facial-Recognition-Tech-Report.pdf>. <<

[42] Ben Gilbert, «Facial-recognition software fails to correctly identify people “96% of the time”, Detroit police chief says», *Business Insider* (2020); disponible en <https://www.businessinsider.com/facial-recognition-fails96-of-the-time-detroit-police-chief-2020-6>. <<

[43] «Passport facial recognition checks fail to work with dark skin», BBC (2019); disponible en <https://www.bbc.com/news/technology49993647>; Jim Nash, «A year later and UK passport biometric face scan system still favors white males», *Biometric Update* (2020); disponible en <https://www.biometricupdate.com/202010/a-year-later-and-ukpassport-biometric-face-scan-system-still-favors-white-males>. <<

[44] Alex Hern, «Twitter apologises for “racist” image-cropping algorithm», *The Guardian* (2020); disponible en <https://www.theguardian.com/technology/2020/sep/21/twitter-apologises-for-racist-image-crop ping-algorithm>. <<

[45] Joy Adowaa Buolamwini, «Gender shades. Intersectional phenotypic and demographic evaluation of face datasets and gender classifiers», MIT Libraries, DSpace@MIT, 2017; disponible en <https:// dspace.mit.edu/handle/1721.1/114068>. <<

[46] Cynthia Cook *et al*., «Demographic Effects in Facial Recognition and their Dependence on Image Acquisition. An Evaluation of Eleven Commercial Systems», *IEEE Transactions on Biometrics, Behavior, and Identity Science* (IEEE T-BIOM) (2019); disponible en <https://ieeexplore.ieee.org/ document/8636231>; Shahina Anwarul y Susheela Dahiya, «A Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition Accuracy», *Proceedings of ICRIC 2019* (2019); disponible en <https://link.springer.com/chapter/10.1007%2F9 78-3-030-29407-6_36>. <<

[47] Ídem. <<

[48] Según el índice AI Global Surveillance (AIGS) elaborado por el Carnegie Endowment for International Peace; disponible en <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillancepub-79847>. <<

[49] Ídem. <<

[50] Ídem. <<

[51] Ídem. <<

[52] Según el mapa del AIGS elaborado por el Carnegie Endowment for International Peace; disponible en <https://carnegieendowment.org/ publications/interactive/ai-surveillance>. <<

[53] Jordi Pérez Colomé, «Palantir, misterioso proveedor del Pentágono y la CIA, ofrece a España sus servicios contra el coronavirus»,*El País* (2020); disponible en <https://elpais.com/tecnologia/2020-04-02/palantir-misteriosoproveedor-del-pentagono-y-la-cia-ofrece-a-espana-sus-servicios-contra-elcoronavirus.xhtml#comentarios>. <<

[54] Paul Lewis *et al*., «UK government using confidential patient data in coronavirus response», *The Guardian* (2020); disponible en <https://www.theguardian.com/world/2020/apr/12/uk-government-usingconfidential-patient-data-in-coronavirus-response>. <<

[55] *BOE* núm. 198, de 21 de julio de 2020; disponible en <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-8276>. <<

[56] Ross Andersen, «The Panopticon Is Already Here», *The Atlantic* (2020); disponible en <www.theatlantic.com/magazine/archive/2020/09/ china-ai-surveillance/614197>. <<

[57] Issie Lapowsky, «In 2020, COVID-19 derailed the privacy debate in the U.S.», *Protocol* (2020); disponible en <https://www.protocol.com/ covid-19-privacy-debate>. <<

[58] Lora Jones, «I monitor my staff with software that takes screenshots», BBC (2020); disponible en <https://www.bbc.com/news/business-54289152>. <<

[59] Laura Delle Femmine, «Ahora espero que Glovo contrate a todos los trabajadores sin trampas», *El País* (2020); disponible en <https://elpais.com/economia/2020-09-24/ahora-espero-que-glovo-contrate-a-todoslos-trabajadores-sin-trampas.xhtml>. <<

[60] Es una de las cuestiones planteadas en el artículo «Plataformas y Gig economy en el trabajo cualificado», publicado en el marco del Congreso Interuniversitario sobre el Futuro del Trabajo de la OIT (2019); disponible en <https://www.ccoo.es/b6d559e4cbdec5c4ce99cd3d0a0dd49a000001.pdf>. <<

[61] Sentencia del Tribunal Ordinario de Bolonia, 31 de diciembre de 2020; disponible en <www.bollettinoadapt.it/wp-content/uploads/2021/ 01/Ordinanza-Bologna.pdf>. <<

[62] Joanna Bronowicka y Mirela Ivanova, «Resisting the Algorithmic Boss. Guessing, Gaming, Reframing and Contesting Rules in App-based Management», *SSRN* (2020); disponible en <https://papers.ssrn.com/sol3/ papers.cfm? abstract_id=3624087>. <<

[63] Como recoge el informe «AI Now 2019 Report» de la organización AI Now; disponible en <https://ainowinstitute.org/AI_Now_ 2019_Report.pdf>. <<

[64] O «code ceiling», como lo denomina Mike Walsh en su artículo «Algorithms Are Making Economic Inequality Worse», *Harvard Business Review* (2020); disponible en: <https://hbr-org.cdn.ampproject.org/c/s/ hbr.org/amp/2020/10/algorithms-are-making-economic-inequalityworse>. <<

[65] Mary L. Gray y Siddharth Suri,*Ghost Work. How to Stop Silicon Valley from Building a New Global Underclass*, Boston, Houghton Mifflin, 2019. <<

[66] «Data Engineering, Preparation and Labeling for AI 2020», Cognilytica (2020). <<

[67] Véase nota 65. <<

[68] David Gilbert, «Bestiality, Stabbings, and Child Porn. Why Facebook Moderators Are Suing the Company for Trauma», *Vice* (2019); disponible en <https://www.vice.com/en/article/a35xk5/facebook-moderators-aresuing-for-trauma-ptsd>. <<

[69] «YouTube censura vídeos paródicos sobre los negacionistas de la COVID-19 mientras se le escapan vídeos sobre la pandemia que sí desinforman», Maldita (2020); disponible en <https://maldita.es/ malditatecnologia/2020/10/02/youtube-censura-videos-parodicosnegacionistas-covid-19-desinformacion/>. <<

[70] Judith Vives, «Instagram censura la parodia de un desnudo pero no la imagen original», *La Vanguardia* (2020); disponible en <https://www.lavanguardia.com/tecnologia/20201020/484199007411/instagram-cen sura-parodia-desnudo-no-imagen-original.xhtml>. <<

[71] «Don’t delete art», disponible en <https://dontdelete.art/>. <<

[72] Sam Biddle *et al*., «Invisible censorship», *The Intercept* (2020); disponible en <https://theintercept.com/2020/03/16/tiktok-app-mode rators-users-discrimination>. <<

[73] Ídem. <<

[74] Tal y como denunció la coalición #SaveYourInternet (<https://saveyourinternet.eu>), liderada en España por Xnet. Véase «Sobre la aprobación de la Directiva Copyright. No lo llames censura, llámalo Derechos de Autor», Xnet (2019), disponible en <https://xnet-x.net/ aprobacion-directiva-copyright-no-llames-censura-llamalo-derechosautor/%20https://xnet-x.net/aprobacion-directiva-copyright-no-llamescensura-llamalo-derechos-autor/>. <<

[75] *Boletín Oficial de las Cortes Generales* (BOCG), núm. 168, 27 de octubre de 2020, p. 1; disponible en <https://www.congreso.es/public_ oficiales/L14/CONG/BOCG/D/BOCG-14-D-168.PDF>. <<

[76] Procedimiento de actuación contra la desinformación, *BOE*, núm. 292, 5 de noviembre de 2020; disponible en: <https://www.boe.es/eli/es/o/2020/10/30/pcm1030/dof/spa/pdf>. <<

[77] «Por qué un Gobierno no debe decidir qué es verdad y qué no y por qué la lucha contra la desinformación no se puede hacer desde órganos no independientes del Gobierno», Maldita (2020); disponible en <https:// maldita.es/nosotros/2020/11/06/gobierno-verdad-no-lucha-desin formacion/>. <<

[78] «Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014», Tribunal de Justicia de la Unión Europea, 2014; disponible en <www.curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES>. <<

[79] «Derecho de supresión (“al olvido”). Buscadores de internet», Agencia Española de Protección de Datos (AEPD), 2020; disponible en <https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/ derecho-al-olvido>. <<

[80] Tribunal Constitucional (*BOE* núm. 164, de sábado 7 de julio de 2018; disponible en: <https://www.boe.es/boe/dias/2018/07/07/pdfs/ BOE-A-2018-9534.pdf>. <<

[81] «Derecho al olvido. Cinco años», Agencia EFE (2019); disponible en <https://www.efe.com/efe/espana/efefuturo/derecho-al-olvido-cincoanos/50000905-3973763>. <<

[82] Como comenta Gemma Galdon Clavell, experta en protección de datos, fundadora de Eticas Research & Consulting y Eticas Foundation, entrevistada en múltiples ocasiones. <<

[83] Todas las excepciones mencionadas se recogen en el apartado 3 del artículo 17 del Reglamento General de Protección de Datos (RGPD), publicado en el *BOE* el 4 de mayo de 2016; disponible en <https://www. boe.es/doue/2016/119/L00001-00088.pdf>. <<

[84] Según explica Dev Lewis, estudioso de la Universidad de Pekín (China) y líder del programa Digital Asia Hub, en su ensayo «Separating Myth From Reality. How China's Social Credit System uses public data for social governance», publicado por Nesta en el marco del informe «The AI Powered State. China's approach to public sector innovation» (2020); disponible en <https://media.nesta.org.uk/documents/Nesta_ TheAIPoweredState_2020.pdf>. <<

[85] En concreto, del episodio 1 de la temporada 3 de *Black Mirror*, «Caída en picado» (Joe Wright, 2016). <<

[86] Lewis, «Separating Myth From Reality…». <<

[87] Ídem. <<

[88] Ídem. <<

[89] Ídem. <<

[90] Ídem. <<

[91] En 2018, el 83 por ciento de todos los pagos efectuados en China fueron móviles, según datos de Statista. Yihan Ma, «Mobile payment market share in China 2011-2018», Statista (2020); disponible en <https://www.statista.com/statistics/1050151/china-market-share-of-mobile-payments/>. <<

[92] Ross Andersen, «The Panopticon Is Already Here», *The Atlantic* (2020); disponible en <www.theatlantic.com/magazine/archive/2020/09/ china-ai-surveillance/614197>. <<

[93] Según datos recopilados por CompariTech y analizados por PreciseSecurity.com. Referencias: «Top 10 Countries and Cities by Number of CCTV Cameras», PreciseSecurity (2019); disponible en <https://www.precisesecurity.com/articles/Top-10-Countries-by-Number-of-CCTVCameras>.
«Surveillance camera statistics. Which cities have the most CCTV cameras?», Comparitech (2020); disponible en <https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/>. <<

[94] «Renfe pone en marcha un proyecto piloto para controlar el aforo en las estaciones de Cercanías en tiempo real», Renfe (2020); disponible en <https://saladeprensa.renfe.com/renfe-pone-en-marcha-un-proyecto-pilotopara-controlar-el-aforo-en-las-estaciones-de-cercanias-en-tiempo-real/>. <<

[95] Michael Mcloughlin, «Origen étnico, sexo o vestimenta. El polémico sistema de Renfe para vigilar a sus viajeros»,*El Confidencial* (2021); disponible en <https://www.elconfidencial.com/tecnologia/2021-02-17/ renfe-videovigilancia-pliego-condiciones-tecnicos_2953824/>. <<

[96] Jamie Bartlett, *The People vs Tech. How the Internet is Killing Democracy (and How We Save It)*, Nueva York, Penguin Random House, 2018. <<

[97] Joseph Menn, «Exclusive. Apple dropped plan for encrypting backups after FBI complained», Reuters (2020); disponible en <https:// www.reuters.com/article/us-apple-fbi-icloud-exclusive/exclusive-appledropped-plan-for-encrypting-backups-after-fbi-complained-sourcesidUSKBN1ZK1CT>. <<

[98] Patrick Howell O’Neill, «US senators on encryption back doors. “We will impose our will” on Apand Facebook», *MIT Technology Review* (2019); disponible en <https://www.technologyreview.com/2019/12/10/ 131634/us-senators-on-encryption-backdoors-we-will-impose-our-willon-apple-and-facebook/>. <<

[99] «Council Resolution on Encryption – Security through encryption and security despite encryption», 2020; disponible en <https:// data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/ pdf>. <<

[100] «The Rise of Central Bank Digital Currencies», Atlantic Council, 2021; disponible en <https://www.atlanticcouncil.org/blogs/econographics/the-rise-of-central-bank-digital-currencies/>. <<

[101] Shoshana Zuboff, *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder*, trad. de Albino Santos, Barcelona, Paidós, 2020. <<

[102] Véase nota 99. <<

[103] Ídem. <<

[104] Eileen Yu,«Singapore police can access COVID-19 contact tracing data for criminal investigations», *ZDNet* (2021); disponible en <https://www.zdnet.com/article/singapore-police-can-access-covid-19-contacttracing-data-for-criminal-investigations/>. <<

[105] «You can log out, but you can never leave. How Amazon manipulates consumers to keep them subscribed to Amazon Prime», Consejo de Consumidores de Noruega, 2021; disponible en <https://fil. forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-canlog-out-but-you-can-never-leave-final.pdf>. <<

[106] Carta de Public Citizen, Campaign for a Commercial-Free Childhood, Center for Digital Democracy, Center for Economic Justice, Consumer Federation of America, Electronic Privacy Information Center y U.S. PIRG a la FTC, 14 de enero de 2021; disponible en <https:// www.citizen.org/wp-content/uploads/Amazon-Dark-Patterns-FTCletter-.pdf>. <<

[107] Reflexión de la científica y académica de la Real Academia de Ingeniería Nuria Oliver, directora de uno de los centros del European Laboratory for Learning and Intelligent Systems (ELLIS) durante nuestra entrevista en 2019 (Esther Paniagua, «Llevo 20 años investigando la inteligencia artificial. Esto es lo que he aprendido y estos serán sus desafíos futuros», *Xataka* (2019); disponible en <https://www.xataka.com/roboticae-ia/llevo-20-anos-investigando-inteligencia-artificial-esto-que-heaprendido-estos-seran-sus-desafios-futuros>). <<

[1] Tim Berners-Lee, «Thirty years after he invented the World Wide Web, Tim Berners-Lee says we all must act to save it», *Quartz* (2019); disponible en <https://qz.com/1568798/tim-berners-lees-annual-letteron-the-world-webs-30th-anniversary/>. <<

[2] Como dijo el propio Tim Berners-Lee durante su discurso para anunciar la creación de la W3F Foundation (2008); disponible en <https:// vimeo.com/1761434>. <<

[3] Ídem. <<

[4] Tim Berners-Lee, «Thirty years after he invented the World Wide Web, Tim Berners-Lee says we all must act to save it», *Quartz* (2019); disponible en <https://qz.com/1568798/tim-berners-lees-annual-letteron-the-world-webs-30th-anniversary/>. <<

[5] La siguiente relación de derechos vulnerados *online* y el concepto de privacidad como «derecho portal» se deducen de forma obvia del contenido de los capítulos anteriores del libro, si bien esta síntesis forma parte de la participación de la experta Gemma Galdon Clavell en el ciclo «La gobernanza de la inteligencia artificial en el mundo pos-COVID-19. Responsabilidad social, democracia y cooperación transnacional», organizado por Globernance, que yo misma relato en el siguiente *podcast*: <https://palaumacaya.org/es/p/la-gobernanza-de-la-inteligencia-artificialen-el-mundo-poscovid19_c13504270>, así como en al artículo «El reconocimiento facial necesita una cuarentena», *El Español* (2021); disponible en <https://www.elespanol.com/invertia/disruptores-innovadores/opinion/20210403/reconocimiento-facial-necesita-cuarentena/570572939_13.html>. <<

[6] Según el informe anual del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) «La sociedad en red. Transformación digital en España», 2019; disponible en <https://www. ontsi.red.es/sites/ontsi/files/2019-10/InformeAnualLaSociedadEn RedEdic2019.pdf>. <<

[7] «World Social Report 2020. Inequality in a rapidly changing world», ONU, 2020; disponible en <https://www.un.org/development/desa/dspd/ wp-content/uploads/sites/22/2020/01/World-Social-Report-2020FullReport.pdf>. <<

[8] Según un análisis del sindicato UGT basado en datos publicados por el Ministerio de Economía; disponible en <https://www.ugt.es/13millones-de-personas-y-26767-poblaciones-en-espana-sin-internet>. <<

[9] Según el informe «Digital Economy and Society Index Report 2020 – Human Capital», Comisión Europea, 2020; disponible en <https:// ec.europa.eu/digital-single-market/en/human-capital>. <<

[10] Según el informe «La brecha digital en España» de UGT. <<

[11] Según el estudio «Hábitos en el uso del móvil en las familias», Durcal, 2021. <<

[12] Ídem. <<

[13] Ídem. <<

[14] Según el informe «Empowering women in the digital age. Where do we stand?», Organisation for Economic Co-operation and Development (OECD), 2018; disponible en <https://www.oecd.org/digital/empoweringwomen-in-the-digital-age-brochure.pdf>. <<

[15] Ídem. <<

[16] «Bridging the gender divide», International Telecommunication Union (ITU), 2019; disponible en <https://www.itu.int/en/mediacentre/backgrounders/Pages/bridging-the-gender-divide.aspx>. <<

[17] «The gender gap in internet access. Using a women-centred method», Web Foundation, 2020; disponible en <https://webfoundation.org/2020/03/the-gender-gap-in-internet-access-using-a-women-centredmethod/>. <<

[18] Véase nota 11 de este mismo capítulo. <<

[19] Josh Jacobs, «Macho “brogrammer” culture still nudging women out of tech», *Financial Times* (2018); disponible en <https://www.ft.com/ content/5dd12c50-dd41-11e8-b173-ebef6ab1374a>. <<

[20] Entrevista a María Sefidari el 7 de febrero de 2020. Como se aprecia en las estadísticas de uso de internet en 1996 del Pew Research Center, disponibles en <https://www.pewresearch.org/politics/1996/12/16/online-use/>. <<

[21] Entrevista a María Sefidari el 7 de febrero de 2020. <<

[22] Adrienne Massanari, «#Gamergate and The Fappening. How Reddit's algorithm, governance, and culture support toxic technocultures», *New Media & Society* (2015); disponible en <https://journals.sagepub.com/ doi/abs/10.1177/1461444815608807>. <<

[23] Ídem. <<

[24] Víctor Navarro, «Feminismo, medios y #GamerGate. Por qué está en guerra el mundo de los videojuegos», *Verne, El País* (2014); disponible en <https://verne.elpais.com/verne/2014/11/02/articulo/1414911892_ 000081.xhtml>. <<

[25] Laura Favaro, «Los estudios críticos de internet. Conceptos, debates y retos», *Teknokultura* (2018); disponible en <https://revistas.ucm.es/index.php/TEKN/article/view/56687/4564456547157>. <<

[26] «Web inventor Sir Tim Berners-Lee responds to US net neutrality threat», W3F, 2017; disponible en <https://webfoundation.org/2017/04/sir-tim-berners-lee-responds-to-us-net-neutrality-threat/>. <<

[27] «In the Matter of Restoring Internet Freedom», 2017; disponible en <https://static.tumblr.com/unowjew/1b8p0vnxq/comments_of_ internet_engineersfcc_nn.pdf>. <<

[28] «Loss of net neutrality could harm research», *Nature* (2017); disponible en <https://www.nature.com/articles/d41586-017-07842-0>. <<

[29] Según datos del estudio «The Net Neutrality Situation in the EU. Evaluation of the First Two Years of Enforcement» (2019) de la red europea para la defensa de los derechos y libertades *online* EDRi; disponible en <https://epicenter.works/sites/default/files/2019_netneutrality_in_euepicenter.works-r1.pdf >. <<

[30] Ídem para los datos aportados en esta línea y en párrafos siguientes. <<

[31] J. Clement, «Google, Amazon, Facebook, Apple, and Microsoft (GAFAM) – statistics & facts», Statista (2020); disponible en <https://www.statista.com/topics/4213/google-apple-facebook-amazon-and-microsoftgafam/>. <<

[32] Mónica Mena Roa, «Los gigantes tecnológicos resisten ante la crisis del coronavirus», Statista (2020); disponible en <https://es.statista.com/grafico/21659/ingresos-de-empresas-tecnologicas-seleccionadas-enel-primer-trimestre-de-2020/>. <<

[33] Shelley E. Kohan, «Amazon’s Net Profit Soars 84% With Sales Hitting $386 Billion», *Forbes* (2021); disponible en <https://www.forbes.com/sites/shelleykohan/2021/02/02/amazons-net-profit-soars-84-withsales-hitting-386-billion/?sh=18b790bc1334>. <<

[34] «Google owner Alphabet sees record growth as ad spend soars», BBC (2021); disponible en <https://www.bbc.com/news/business-559 13453>. <<

[35] Chris Welch, «Apple surpasses $100 billion in quarterly revenue for first time in its history», *The Verge* (2021); disponible en <https://www.theverge.com/2021/1/27/22252663/apple-q1-2021-earnings-iphone-12mac-sales>. <<

[36] «The new rules of competition in the technology industry», *The Economist* (2021); disponible en <https://www.economist.com/business/ 2021/02/27/the-new-rules-of-competition-in-the-technologyindustry>. <<

[37] «Bloomberg Billionaires Index View», Bloomberg (2021); disponible en <https://www.bloomberg.com/billionaires/>. <<

[38] Carta de Netflix a los accionistas de la compañía, 21 de enero de 2021; disponible en <https://s22.q4cdn.com/959853165/files/doc_financials/2020/q4/FINAL-Q420-Shareholder-Letter.pdf>. <<

[39] Fernando García, «Netflix duplica beneficios y dispara el número de abonados por la pandemia», *La Vanguardia* (2020); disponible en <https://www.lavanguardia.com/cultura/20200422/48677811708/netflix-duplicabeneficios-pandemia.xhtml>. <<

[40] Autor de *Cómo creamos internet* (Barcelona, Península, 2013) y expresidente de la Internet Society, entre otros muchos cargos. <<

[41] Cecilia Kang y Mike Isaac, «U. S. and States Say Facebook Illegally Crushed Competition»,*The New York Times* (2020); disponible en <https:// www.nytimes.com/2020/12/09/technology/facebook-antitrust-mono poly.xhtml>. <<

[42] «Antitrust. Commission fines Google –4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine», Comisión Europea, 2018; disponible en: <https://ec.europa.eu/commission/presscorner/detail/en/IP_ 18_4581>. <<

[43] «Epic Game Files EU Antitrust Complaint Against Apple», Epic Games (2021); disponible en <https://www.epicgames.com/site/en-US/ news/epic-games-files-eu-antitrust-complaint-against-apple>. <<

[44] Tal y como explicaba Ángel Gómez de Ágreda, jefe del Área de Análisis Geopolítico de la División de Coordinación y Estudios de Seguridad y Defensa de la Secretaría General de Política de Defensa (SEGENPOL, Ministerio de Defensa) y autor de *Mundo Orwell. Manual de supervivencia para un mundo hiperconectado* (Barcelona, Ariel, 2019), durante nuestra entrevista el 3 de marzo de 2020. <<

[45] España es el país de la Unión Europea con la mayor tasa de penetración de fibra óptica hasta el hogar (Fiber To The Home [FTTH]), según el informe «2020 Market Panorama», FTTH Council Europe, 2020; disponible en <https://www.ftthcouncil.eu/documents/FTTH%20Co uncil%20Europe%20-%20Panorama%20at%20September%202019%20 -%20Webinar%20Version4.pdf>. <<

[46] Según el informe «European Digital Sovereignty», OliverWyman, 2020. <<

[47] Ídem. <<

[48] Según datos de Statcounter; disponibles en <https://gs.statcounter.com/search-engine-market-share/all/russian-federation>. <<

[49] Kai-Fu Lee, *Superpotencias de la inteligencia artificial. China, Silicon Valley y el nuevo orden mundial*, trad. de Mercedes Vaquero Granados, Barcelona, Deusto, 2020. <<

[1] La carta ahora se titula «G is for Google» y es el texto de presentación de la web de Alphabet, disponible en <https://abc.xyz/>. <<

[2] Davide Castelvecchi, «AI pioneer.“The dangers of abuse are very real”», *Nature* (2019); disponible en <https://www.nature.com/articles/ d41586-019-00505-2>. <<

[3] Es una de las conclusiones de un demoledor informe del Digital, Culture, Media and Sport Committee del Reino Unido, publicado en 2019 y disponible en <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>. <<

[4] Como se explica en el cap.8, GAFAM (Google, Amazon, Face-book, Apple y Microsoft) y BAT (Baidu, Alibaba y Tencent) son las siglas que engloban a los gigantes tecnológicos de Estados Unidos (en el primer caso) y de China (en el segundo). <<

[5] Alain Supiot, véanse notas 105 y 106 del cap. 7. <<

[6] Daniel Innerarity, «La pandemia de los datos», *El País* (2021); disponible en <https://elpais.com/opinion/2021-01-21/la-pandemia-delos-datos.xhtml>. <<

[7] «Let us breathe! Censorship and criminalization of online expression in Viet Nam», Amnesty International (2020); disponible en <https://www.amnesty.org/download/Documents/ASA4132432020ENGLISH.pdf>.
<<

[8] «Facebook Transparency Report», Facebook, 2020; disponible en <https://transparency.facebook.com>. <<

[9] «Facebook, YouTube accused of complicity in Vietnam rights abuses», Al Jazeera (2020); disponible en <https://www.aljazeera.com/ news/2020/12/1/facebook-youtube-accused-on-complicity-in-vietnamrights-abuses>. <<

[10] Ídem. <<

[11] James Harkin, *Mobilisation. The growing public interest in mobile technology*, Londres, Demos, 2003; disponible en <http://www.demos.co.uk/files/Mobilisation.pdf>. <<

[12] Según me explicaba el psiquiatra y profesor emérito de la Universidad de California en San Diego (Estados Unidos) Saul Levine para un reportaje publicado en *Buena Vida*, *El País* (2017); disponible en <https://elpais.com/elpais/2017/11/06/buenavida/1509965411_556909.xhtml>. <<

[13] Como señala José Manuel Sánchez, codirector del Centro de Estudios del Coaching. <<

[14] «Technology adoption in US households, 2005 to 2019», Our World in Data (2019); disponible en <https://ourworldindata.org/grapher/ technology-adoption-by-households-in-the-united-states?tab=chart&stac
kMode=absolute&time=2005..2019&country=~Social%20media%20
usage&region=World>. <<

[15] En 2018 Facebook tenía 2.260 millones de usuarios, y en 2008 tenía cien millones (<https://ourworldindata.org/grapher/users-by-socialmedia-platform?time=2008..2019&country=~Facebook>); la población mundial en 2008 era de 6.800 millones y en 2018 de 7.630 millones (<https://ourworldindata.org/grapher/world-population-by-worldregions-post-1820>), según datos de Our World in Data. <<

[16] Tal y como lo define Sinan Aral en *The Hype Machine*, Londres, HarperCollins, 2020. <<

[17] Brian A. Primack *et al*., «Social Media Use and Perceived Social Isolation Among Young Adults in the U. S.», *American Journal of Preventive Medicine* (2017); disponible en <https://www.ajpmonline.org/article/ S0749-3797(17)30016-8/fulltext>. <<

[18] Entrevista de Jordi Évole a Zygmunt Bauman: «Se dio cuenta de que nuestra peor pesadilla es ser abandonados», *Salvados* (2017); disponible en <https://www.youtube.com/watch?v=_EnGbibIGx4>. <<

[19] Ricardo de Querol, «Zygmunt Bauman.“Las redes sociales son una trampa”», *El País* (2016); disponible en <https://elpais.com/cultura/2015/12/30/babelia/1451504427_675885.xhtml>. <<

[20] Tal y como señalaba Ángel Gómez de Ágreda, jefe del Área de Análisis Geopolítico de la División de Coordinación y Estudios de Seguridad y Defensa de la Secretaría General de Política de Defensa (SEGENPOL, Ministerio de Defensa) y autor de *Mundo Orwell. Manual de supervivencia para un mundo hiperconectado* (Barcelona, Ariel, 2019), durante nuestra entrevista el 3 de marzo de 2020. <<

[21] Maksym Gabielkov, «Social Clicks. What and Who Gets Read on Twitter?», *ACM Sigmetrics* (2016); disponible en <https://dl.acm.org/doi/10.1145/2964791.2901462>. <<

[22] Annie Reneau, «I wrote a news headline that didn’t even link to a story. Over 2,000 people commented on it anyway», *Upworthy* (2019); disponible en <https://www.upworthy.com/comments-didnt-read-thearticle>. <<

[23] Véanse Marc Hooghe y Jennifer Oser, «Internet, television and social capital. The effect of “screen time” on social capital», *Information, Communication & Society* (2015); disponible en <https://doi.org/ 10.1080/1369118X.2015.1022568>; B. Veenhof *et al*., «How Canadians’ Use of the Internet Affects Social Life and Civic Participation», Science, Innovation and Electronic Information Division (SIEID), Ottawa, Canadá, 2008; disponible en <https://www150.statcan.gc.ca/n1/en/pub/56f0004m/56f0004m2008016-eng.pdf?st=UUXUiWEk>. <<

[24] Como muestra el estudio liderado por el matemático Esteban Moro en el marco del proyecto «Atlas de la desigualdad», disponible en <https://inequality.media.mit.edu/>. <<

[25] Como apunta José María Lassalle en *Ciberleviatán*, Barcelona, Arpa, 2019. <<

[26] Es el análisis de Lorena Jaume-Palasí, fundadora de Ethical Tech Society, expuesto durante nuestra entrevista el 22 de julio de 2020. <<

[27] Ídem (véase nota 26, cap. 6). <<

[28] Como discurre Lorena Jaume-Palasí, fundadora de Ethical Tech Society, entrevistada el 22 de julio de 2020. <<

[29] Según la versión oficial de Google, fue ella quien dimitió al no haber cumplido Google con las condiciones que la investigadora había impuesto para no irse. Para más detalles, véase Casey Newton, «The withering email that got an ethical AI researcher fired at Google», *Platformer* (2020); disponible en: <https://www.platformer.news/p/the-witheringemail-that-got-an-ethical>. <<

[30] Emma Strubell *et al*., «Energy and Policy Considerations for Deep Learning in NLP», *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics* (2019); disponible en <https://www.aclweb.org/ anthology/P19-1355.pdf>. <<

[31] Informe «Data Centres and Data Transmission Networks», International Energy Agency (IEA), 2020; disponible en <https://www.iea.org/reports/data-centres-and-data-transmission-networks>. <<

[32] Las cifras varían según las metodologías usadas para las mediciones y pronósticos. Véase Anders S. G. Andrae, «On Global Electricity Usage of Communication Technology. Trends to 2030», *Challenges* (2015); disponible en <https://doi.org/10.3390/challe6010117> ; «ICT Carbon footprint», European Framework Initiative for Energy & Environmental Efficiency in the ICT Sector; disponible en <https://ictfootprint.eu/en/about/ictcarbon-footprint/ict-carbon-footprint>; Anders S. G. Andrae, «New perspectives on internet electricity use in 2030», *Engineering and Applied Science Letter* (2020); disponible en <https://pisrt.org/psr-press/journals/easlvol-3-issue-2-2020/new-perspectives-on-internet-electricity-usein-2030/>. <<

[33] Estimaciones del estudio de Anders S. G. Andrae de 2015, revisadas en 2020. Véanse fuentes en la nota anterior. <<

[34] Informe «The Global Internet Phenomena Report», Sandvine (2020); disponible en <https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2020/Phenomena/COVID%20Internet%20Phenomena%20Report%2020200507.pdf>. <<

[35] Informe «Cisco Annual Internet Report (2018-2023) White Paper», Cisco (2020); disponible en <https://www.cisco.com/c/en/us/ solutions/collateral/executive-perspectives/annual-internet-report/whitepaper-c11-741490.xhtml>. <<

[36] Ídem. <<

[37] Informe «Lean ICT. Towards Digital Sobriety», The Shift Project (2019); disponible en <https://theshiftproject.org/wp-content/uploads/ 2019/03/Lean-ICT-Report_The-Shift-Project_2019.pdf>. Véase también nota 33 de este capítulo. <<

[38] En total, más de un 55 por ciento en 2019, que ascendió a un 57,64 por ciento en los primeros meses de 2020, según el informe de Sandvine (véase nota 34 de este capítulo). <<

[39] Es un cálculo conservador si se tiene en cuenta el posible margen de error en el total de emisiones del sector TIC proyectado para 2020 (687 millones de toneladas) según el informe «Trayectorias de emisiones de gases de efecto invernadero para el sector de las TIC compatibles con el Acuerdo de París de la CMNUCC», Unión Internacional de Telecomunicaciones (2020); disponible en <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14084>. <<

[40] Las emisiones netas en España en 2019 fueron de 276.904,3 millones de toneladas, según la Resolución de la Dirección General de Calidad y Evaluación Ambiental de Aprobación del Inventario Nacional de Emisiones a la Atmósfera para la serie 1990-2019 (edición de 2021), publicada en 2020 por el Ministerio para la Transición Ecológica y el Reto Demográfico; disponible en <https://www.miteco.gob.es/es/calidad-y-evaluacion-ambiental/temas/sistema-espanol-de-inventario-sei-/resolucionaprobacioninventario2021_tcm30-520469.pdf>. <<

[41] Christian Stoll *et al*., «The Carbon Footprint of Bitcoin», *Joule* (2019); disponible en <https://www.cell.com/joule/fulltext/S2542-4351 (19)30255-7>. <<

[42] George Kamiya, «Bitcoin energy use – mined the gap», International Energy Agency (IEA) (2019); disponible en <https://www.iea.org/commen taries/bitcoin-energy-use-mined-the-gap>. <<

[43] Alex de Vries, «Bitcoin’s energy consumption is underestimated. A market dynamics approach», *Energy Research & Social Science* (2020); disponible en <https://doi.org/10.1016/j.erss.2020.101721>. <<

[44] Según el Bitcoin Energy Consumption Index (BECI), 8 de febrero de 2021 (véase <https://digiconomist.net/bitcoin-energy-consumption>). <<

[45] «Bitcoin consumes “more electricity than Argentina”», BBC (2021); disponible en <https://www.bbc.com/news/technology-56012952>. <<

[46] Ídem. <<

[47] Las emisiones brutas de gases de efecto invernadero en Nueva Zelanda en 2018 fueron de 78,9 millones de toneladas. Véase «New Zealand's Greenhouse Gas Inventory», 2020, según el ministerio neozelandés para el Medio Ambiente, disponible en <https://www.mfe.govt.nz/ climate-change/state-of-our-atmosphere-and-climate/new-zealands-green house-gas-inventory#:~:text=New%20Zealand's%20gross%20green house%20gas%20emissions%20in%202018%20were%2078.9, decreased%20 by%201%20per%20cent>. <<

[48] Según el Cambridge Bitcoin Electricity Consumption Index (CBECI); disponible en <https://cbeci.org>. <<

[49] Según el análisis de South Pole para el proyecto CleanCoin; disponible en <http://www.cleancoins.io/files/cleancoin/factsheet.pdf>. <<

[50] Camilo Mora *et al*., «Bitcoin emissions alone could push global warming above 2 °C», *Nature Climate Change* (2018); disponible en <https://www.nature.com/articles/s41558-018-0321-8>. <<

[51] Ídem. <<

[52] «Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares», INE, 2020; disponible en <https://www.ine.es/prensa/tich_2020.pdf>. <<

[53] Según el Estudio Anual de eCommerce 2020 de IAB, disponible en <https://iabspain.es/download/41528/>. <<

[54] Sadegh Shahmohammad *et al*., «Comparative Greenhouse Gas Footprinting of Online versus Traditional Shopping for Fast-Moving Consumer Goods. A Stochastic Approach», *Environmental Science and Technology* (2020); disponible en <https://pubs.acs.org/doi/pdf/10.1021/acs.est.9b06252>. <<

[55] «Global E-Waste – Statistics & Facts», Statista (2020); disponible en <https://www.statista.com/topics/3409/electronic-wasteworldwide/#:~:text=In%202018%2C%20just%2020%20percent,metric%20tons%20was%20produced%20worldwide.&text=However%2C%20e-waste%20generation%20per,developed%20nations%20in%20the%20 west>. <<

[56] Ídem. <<

[57] José Luis Sanz, «Italia condena a Apple por la obsolescencia programada en sus iPhone», *Cinco Días* (2020); disponible en <https://cincodias.elpais.com/cincodias/2020/06/01/lifestyle/1590995739_ 694167.xhtml>. <<

[58] «Apple pagará unos 25 dólares a los usuarios de iPhone afectados por la obsolescencia programada en EE UU», Europa Press (2020); disponible en <https://www.europapress.es/portaltic/sector/noticia-apple-pagara25-dolares-usuarios-iphone-afectados-obsolescencia-programadaeeuu-20200713183734.xhtml>. <<

[59] Según el informe «La perspectiva mundial sobre la diversidad biológica 5», Secretaría del Convenio sobre la Diversidad Biológica (CBD) (ONU), 2020; disponible en <https://www.cbd.int/gbo/gbo5/publication/ gbo-5-es.pdf>. <<

[60] Karn Vohra *et al*., «Global mortality from outdoor fine particle pollution generated by fossil fuel combustion. Results from GEOS-Chem», *Environmental Research* (2021); disponible en <https://doi.org/10.1016/j. envres.2021.110754>. <<

[61] Declaraciones de David Cooper a *The New YorkTimes*. Véase Catrin Einhorn, «A “Crossroads” for Humanity. Earth’s Biodiversity Is Still Collapsing»,*The New York Times* (2020); disponible en <https://www.nytimes.com/2020/09/15/climate/biodiversity-united-nations-report.xhtml>. <<

[62] Véase nota 25, de este capítulo. <<

[63] Shoshana Zuboff, *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder*, trad. de Albino Santos, Barcelona, Paidós, 2020. <<

[64] Jill Lepore, «A Golden Age for Dystopian Fiction», *The New Yorker* (2017); disponible en <https://www.newyorker.com/magazine/2017/06/ 05/a-golden-age-for-dystopian-fiction>. <<

[65] Disponible en <https://www.economist.com/the-world-if/>. <<

[1] Andrew Perrin, «Americans Are Changing Their Relationship with Facebook», Pew Research Center, 2018; disponible en <www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/>. <<

[2] Histórico de valores en bolsa de Facebook, 2020, Yahoo Finance; disponible en <https://finance.yahoo.com/quote/FB/history?period1= 1521158400&period2 =1522108800&interval=1d&filter=history&frequency=1d&includeAdjusted Close=true>. <<

[3] «FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook», FTC, 2019; disponible en <https://www.ftc.gov/ news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.
<<

[4] California Consumer Privacy Act of 2018; disponible en <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>. <<

[5] Mike Isaac, «Uber C. E. O. to Leave Trump Advisory Council After Criticism», *The New York Times* (2017); disponible en <https://www.nytimes.com/2017/02/02/technology/uber-ceo-travis-kalanick-trump-advisory-council.xhtml>. <<

[6] Ian Sample, «The great project. How Covid changed science for ever»,*The Guardian* (2020); disponible en <https://www.theguardian.com/world/2020/dec/15/the-great-project-how-covid-changed-science-forever>. <<

[7] Artículo sobre la Wikipedia publicado en la Wikipedia (actualizado el 21 de enero de 2021); disponible en <https://en.wikipedia.org/wiki/ Wikipedia#cite_note-Econ21-6>. <<

[8] «About the Internet Archive», Internet Archive, <https://archive.org/about/>. <<

[9] La controversia alrededor de Richard Stallman no tiene que ver con su defensa del *software* libre, sino con sus comentarios en defensa de la pedofilia y la pornografía infantil, además de ofensas contra personas con discapacidad y acusaciones de actitudes sexistas contra las mujeres. Por todo ello tuvo que dejar la presidencia de la Fundación del Software Libre (FSF) que él mismo fundó, a cuyo comité de dirección regresó en 2021 no sin polémica. Véase Edward Ongweso Jr., «Famed Computer Scientist Richard Stallman Described Epstein Victims As "Entirely Willing"», *Vice* (2019), disponible en <https://www.vice.com/en/article/9ke3ke/famed-computer-scientist-richard-stallman-described-epstein-victims-as-entirely-willing>; «Richard Stallman's personal political notes from 2003: May – August», disponible en <https://stallman.org/archives/2003-may-aug.xhtml>; «Richard Stallman's personal political notes from 2006: March – June», disponible en <https://stallman.org/archives/2006-mar-jun.html#05%20June%202006%20%28Dutch%20paedophiles%20form%20political%20party%29>; «Richard Stallman's personal political notes from 2012: July – October», disponible en <https://stallman.org/archives/2012-jul-oct.html#15_September_2012_%28Censorship_of_child_pornography%29>; Danny O'Brien, «Statement on the Re-election of Richard Stallman to the FSF Board», Electronic Frontier Foundation (EFF) (2021), disponible en <https://www.eff.org/es/deeplinks/2021/03/statement-re-election-richard-stallman-fsf-board>. <<

[10] Richard Stallman, «El *software* libre es ahora aún más importante», GNU, 2013; disponible en <https://www.gnu.org/philosophy/freesoftware-even-more-important.xhtml>. <<

[11] «European Commission Open Source Study», 2021, FraunhoferInstitut y OpenForum Europe; disponible en <https://openforumeurope.org/wp-content/uploads/2021/02/Summit-Study-Presentation.pdf>. <<

[12] Como señala Mara Balestrini, experta en interacción humanocomputadora, cofundadora de Salus-Coop y exdirectora de Ideas for Change. Entrevista realizada el 10 de febrero de 2021. <<

[13] Ídem. <<

[14] Mara Balestrini, «A City in Common Explorations on Sustained Community Engagement with Bottom-up Civic Technologies», University College London, 2017; disponible en <https://discovery.ucl.ac.uk/id/ eprint/1547540/>. <<

[15] Paula Forteza, «The future of Digital Democracy», Citizenlab, 2020; disponible en <https://docsend.com/view/afwdxfw>. <<

[16] Aelita Skaržauskienė y Monika Mačiulienė, «Mapping International Civic Technologies Platforms», *Informatics* (2020); disponible en <https://doi.org/10.3390/informatics7040046>. <<

[17] «Informe de Impacto 2018», Change.org (2019); disponible en <https://static.change.org/brand-pages/impact/reports/2019/change.org_Impact_Report_spanish_FINAL.pdf>. <<

[18] Véase nota 23, cap. 9. <<

[19] Ídem. <<

[20] Iniciativa coordinada desde Fablab Barcelona por Mara Balestrini, en el marco del proyecto europeo Making Sense, <http://making-sense.eu/ campaigns/placa-del-sol/>. <<

[21] Solo la guía «The Civic Tech Field Guide» (<https://civictech.guide/>) recoge más de cuatro mil. <<

[22] Véase nota 23, cap. 9. <<

[23] Samuel Bowles y Jung-Kyoo Choib, «Coevolution of farming and private property during the early Holocene», *Proceedings of the National Academy of Sciences (PNAS)* (2013); disponible en <https://www.pnas.org/content/pnas/110/22/8830.full.pdf>. <<

[24] «Los modelos colaborativos y bajo demanda en plataformas digitales», Adigital y Sharing España, 2017. <<

[25] Ídem. <<

[26] Ídem. <<

[27] Rachel Botsman y Roo Rogers, «Más allá de Zipcar. Consumo colaborativo», *Harvard Business Review* (2011); disponible en <https://hbr.org/2010/10/beyond-zipcar-collaborative-consumption?language=es>. <<

[28] También según el autor y especialista en economía de plataformas Albert Cañigueral, fundador en 2011 de ConsumoColaborativo.com. <<

[29] Ídem. <<

[30] Madrid, Barcelona, Zaragoza, València, A Coruña y varias ciudades andaluzas son algunas de las urbes españolas que han puesto en marcha presupuestos participativos, si bien se critica la limitación tanto de la capacidad de participación y propuesta ciudadana como de la cantidad presupuestaria sobre la que se puede decidir. <<

[31] Olivera Kostoska y Ljupco Kocarev, «A Novel ICT Framework for Sustainable Development Goals», *Sustainability* (2019); disponible en <https://doi.org/10.3390/su11071961>. <<

[32] J. Wu *et al*., «Information and Communications Technologies for Sustainable Development Goals State-of-the-Art, Needs and Perspectives», IEEE, 2018; disponible en <https://ieeexplore.ieee.org/document/ 8306870>. <<

[33] Ídem. <<

[34] Ídem. <<

[35] Ídem. <<

[1] Shoshana Zuboff, «Facebook, Google and a dark age of surveillance capitalism», *Financial Times* (2019); disponible en <https://www.ft.com/ content/7fafec06-1ea2-11e9-b126-46fc3ad87c65>. <<

[2] Tim Berners-Lee, «Thirty years after he invented the World Wide Web, Tim Berners-Lee says we all must act to save it», *Quartz* (2019); disponible en <https://qz.com/1568798/tim-berners-lees-annual-letteron-the-world-webs-30th-anniversary/>. <<

[3] Así lo relata el abogado Javier de la Cueva, uno de los protagonistas, entrevistado el 25 de febrero de 2021. La historia ha sido corroborada por otros de sus protagonistas y difundida en algunos medios de comunicación. En un artículo en *Wired*, Larry Sanger, el cofundador de la Wikipedia, admitió tímidamente que «la bifurcación de la Wikipedia en español bien podría haber sido la gota que colmó el vaso a favor de una Wikipedia cien por cien libre de publicidad». El otro fundador (Jimmy Wales) dijo que «la bifurcación en español fue un evento importante en la historia de Wikipedia, pero no en el sentido de provocar cambios», y que fue su negativa a aceptar publicidad lo que llevó a Wikipedia a ser como es hoy (Nathaniel Tkacz, «The Spanish Fork. Wikipedia–s ad-fuelled mutiny»,*Wired* [2011]; disponible en <https://www.wired.co.uk/article/wikipedia-spanish-fork>). <<

[4] Según datos del estudio «Actitudes ante la tecnología y usos de las TIC en la sociedad española en el marco del Covid-19», Fundación BBVA, 2021; disponible en <https://www.fbbva.es/wp-content/uploads/2021/02/ Presentacion-Estudio-Usos-Internet-Covid19.pdf>. <<

[5] Véase nota 1 de este capítulo. <<

[6] Ídem. <<

[7] «Testimony before the U. S.-China Economic and Security Review Commission. Hearing on China’s Strategic Aims in Africa», Economic and Security Review Commission de Estados Unidos y China, 2020; disponible en <https://www.uscc.gov/sites/default/files/Feldstein_Testimony.pdf>. <<

[8] Como advierte *The Economist* en «Democracies must team up to take on China in the technosphere», *The Economist* (2020); disponible en <https://www.economist.com/briefing/2020/11/19/democracies-mustteam-up-to-take-on-china-in-the-technosphere>. <<

[9] Como apunta Lorena Jaume-Palasí, fundadora de Ethical Tech Society, entrevistada en varias ocasiones a lo largo de 2019, 2020 y 2021. <<

[10] Lo sugiere Gemma Galdon Clavell, fundadora de Eticas Research Consulting y Eticas Foundation y pionera en la auditoría ética de algoritmos, entrevistada en varias ocasiones a lo largo de 2019, 2020 y 2021. <<

[11] Siguiendo la propuesta del *think tank* Council on Foreign Relations (CFR) en su informe «Weaponizing Digital Trade. Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity», 2020; disponible en <https://cdn.cfr.org/sites/default/files/report_pdf/weaponizing-digitaltrade_csr_combined_final.pdf>. <<

[12] Algo así propone Ian Bremmer, presidente y fundador de la firma de consultoría e investigación de riesgos políticos Eurasia Group, que aboga por crear una Organización Mundial de Datos. Véase Ian Bremmer, «Why we need a World Data Organization. Now», *GZERO* (2019); disponible en <https://www.gzeromedia.com/why-we-need-a-world-data-organization-now>. <<

[13] Es una de las propuestas que la economista y profesora emérita de Harvard Shoshana Zuboff hace durante una entrevista con la editora jefe de *The Markup*, Julia Angwin, publicada en su boletín semanal de noticias el 13 de febrero de 2021. <<

[14] Ídem. <<

[15] Extracto del discurso de Tim Cook durante la conferencia CPDP (Computers, Privacy and Data Protection) el 3 de febrero de 2021; disponible en <https://youtu.be/OaLxTz1Yw7M>. <<

[16] Como plantea el extrabajador de Google James Williams en *Clics contra la humanidad*, trad. de Álex Gibert, Barcelona, Gatopardo Ediciones, 2021. <<

[17] Como bien apunta Carissa Véliz en *Privacidad es poder*, trad. de Albino Santos, Barcelona, Debate, 2021. <<

[18] Tim Hwang, *Subprime Attention Crisis. Advertising and the Time Bomb at the Heart of the Internet*, Nueva York, Farrar, Straus and Giroux, 2020. <<

[19] «EDPS Opinions on the Digital Services Act and the Digital Markets Act», 2021, European Data Protection Supervisor (EDPS); disponible en <https://edps.europa.eu/press-publications/press-news/pressreleases/2021/edps-opinions-digital-services-act-and-digital_en>. <<

[20] Emily Stewart, «Poll. Two-thirds of Americans want to break up companies like Amazon and Google», *Vox* (2019); disponible en <https:// www.vox.com/policy-and-politics/2019/9/18/20870938/break-up-bigtech-google-facebook-amazon-poll>. <<

[21] «Techlash 2020. Why the technology sector needs to lean in now on consumer expectations», FleishmanHillard, 2020; disponible en <https://fleishmanhillard.com/wp-content/uploads/meta/resource-file/2020/ techlash-2020-why-the-technology-sector-needs-to-lean-in-now-onconsumer-expectations-1600287855.pdf>. <<

[22] «Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales)», *Diario Oficial de la Unión Europea* (2020); disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri= CELEX:52020PC0842&from=es>. <<

[23] «Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas)», *Diario Oficial de la Unión Europea* (2017); disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri= CELEX:52017PC0010&from=ES>. <<

[24] Como explica Martin Tisné en «Data isn’t the new oil, it’s the new CO2», Luminate, 2019; disponible en <https://luminategroup.com/posts/ blog/data-isnt-the-new-oil-its-the-new-co2>. <<

[25] Iniciativa descrita con más detalle en el cap. 10. <<

[26] Como señala Javier de la Cueva —abogado, doctor en filosofía y estudioso de las relaciones entre el derecho y la tecnología—, entrevistado el 25 de febrero de 2021; Mark Wilkinson *et al*., «The FAIR Guiding Principles for scientific data management and stewardship», *Nature* (2016); disponible en <https://www.nature.com/articles/sdata201618>. <<

[27] Véase nota 17 de este capítulo. <<

[28] Ibíd. <<

[29] Según el artículo 8 del RGPD, «Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información», *BOE* (2016); disponible en <https://www.boe.es/doue/ 2016/119/L00001-00088.pdf>. <<

[30] Francesco Rodella, «Polémica por la violación del avatar de una niña de siete años en un popular videojuego», *El País* (2018); disponible en <https://elpais.com/tecnologia/2018/07/06/actualidad/153087 1736_133106.xhtml>. <<

[31] Sentencia núm. 123/2020 de 6 de octubre de 2020. Sentencias del Tribunal de Justicia en los asuntos C-511/18, C-512/18, C-520/18, C-623/ 17, Tribunal de Justicia de la Unión Europea, La Quadrature du Net y otros; disponible en <https://curia.europa.eu/jcms/upload/docs/application/ pdf/2020-10/cp200123en.pdf>. <<

[32] Véase nota 15 de este capítulo. <<

[33] Ryan Mac y Craig Silverman, «Facebook Has A Metric For “Violence And Incitement Trends”. It’s Rising», *BuzzFeed* (2020); disponible en <https://www.buzzfeednews.com/article/ryanmac/ facebook-internal-metric-violence-incitement-rising-vote>. <<

[34] Kevin Roose «In Pulling Trump's Megaphone, Twitter Shows Where Power Now Lies», *The New York Times* (2021); disponible en <https://www.nytimes.com/2021/01/09/technology/trump-twitter-ban.html>. <<

[35] «Code of Practice on Disinformation»; disponible en <https://ec.europa.eu/digital-single-market/en/code-practice-disinformation>. <<

[36] Tal y como sugiere Joan Donovan, directora de investigación del Shorenstein Center on Media, Politics and Public Policy de la Harvard Kennedy School y responsable del Technology and Social Change Project (TaSC). <<

[37] Anne Applebaum y Peter Pomerantsev, «How to Put Out Democracy's Dumpster Fire», *The Atlantic* (2021); disponible en <https://www.theatlantic.com/magazine/archive/2021/04/the-internet-doesnt-have-tobe-awful/618079/>. <<

[38] «Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre un mercado único de servicios digitales (Ley de Servicios Digitales) y por la que se modifica la Directiva 2000/31/CE», *Diario Oficial de la Unión Europea* (2020); disponible en <https://eur-lex.europa. eu/legal-content/ES/TXT/PDF/? uri=CELEX:52020PC0825& from=en>. <<

[39] Hannah Arendt, *Between Past and Future. Eight Exercises in Political Thought*, Nueva York, Viking Press, 1977. [Hay trad. cast.: *Entre el pasado y el futuro. Ocho ejercicios sobre la reflexión política*, trad. de Ana Poljak, Barcelona, Península, 2016.] <<

[40] Simona Levi (dir.),*#FakeYou. Fake news y desinformación*, Barcelona, Rayo Verde, 2019. <<

[41] En el momento de escribir esto, en marzo de 2021, Birdwatch es una iniciativa en fase piloto para personas de Estados Unidos. Más información en <https://twitter.github.io/birdwatch/>. <<

[42] Véanse J. Nathan Matias, «Persuading Algorithms with an AI Nudge Fact-Checking Can Reduce the Spread of Unreliable News. It Can Also Do the Opposite», *Medium* (2017), disponible en <https:// medium.com/mit-media-lab/persuading-algorithms-with-an-ai-nudge25c92293 df1d>, y J. Nathan Matias «Nudging Algorithms by Influencing Human Behavior. Effects of Encouraging Fact-Checking on News Rankings Contributors», OSF, 2020, disponible en <https://osf.io/ m98b6/>. <<

[43] En referencia a la «proposición no de ley sobre la prevención de la propagación de discursos de odio en el espacio digital» y al «procedimiento de actuación contra la desinformación», mencionados en el cap. 7. <<

[44] Sentencia ECLI: NL: RBDHA: 2020: 1878, «SyRI legislation in breach of European Convention on Human Rights», Tribunal de La Haya, 2020; disponible en <https://uitspraken.rechtspraak.nl/inziendocument?
id=ECLI:NL:RBDHA:2020:1878>. <<

[45] «Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas arzmonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión», Comisión Europea, 2021; disponible en <https:// eur-lex.europa.eu/resource.xhtml?uri=cellar:e0649735-a372-11eb-958501aa75ed71a1.0008.02/DOC_1&format=PDF>. <<

[46] Como señala el informe «Regulating Biometrics. Global Approaches and Urgent Questions», AINow, 2020; disponible en <https://ainowinstitute.org/regulatingbiometrics.pdf>. <<

[47] Ídem. <<

[48] Ídem. <<

[49] «Estrategia Nacional de Inteligencia Artificial», Gobierno de España, 2020; disponible en <https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIAResumen2B.pdf>. <<

[50] Tal y como propone Cathy O’Neil en *Armas de destrucción matemática. Cómo el big data aumenta la desigualdad y amenaza la democracia*, trad. de Violeta Arranz de la Torre, Madrid, Capitán Swing, 2018. <<

[51] Como reconoce la Comisión Europea y amplía en su documento «Directrices éticas para una IA fiable» (2019); disponible en <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60423>. <<

[52] Ídem. <<

[53] Williams, *Clics contra la humanidad*. <<

[54] Emanuel Derman y Paul Wilmott, «The Financial Modelers' Manifesto», 2009; disponible en <https://www.uio.no/studier/emner/sv/oekonomi/ECON4135/h09/undervisningsmateriale/FinancialModelersManifesto.pdf>. <<

[55] Julian Oliver, Gordan Savičić y Danja Vasiliev, «The Critical Engineering Manifesto», The Critical Engineering Working Group, 2011; disponible en <https://criticalengineering.org/ce.pdf>. <<

[56] Véase nota 52 de este capítulo. <<

[57] Ídem. <<

[58] Según el sindicato Alphabet Workers Union, <https://twitter.com/AlphabetWorkers/status/1346050124544233473>. <<

[59] Carl B. Frey, *The Technology Trap. Capital, Labor, and Power in the Age of Automation*, Princeton (New Jersey), Princeton University Press, 2019. <<

[60] Genís Roca, «Tener trabajo ya no garantiza tener derechos», *VIA Empresa* (2020); disponible en <https://www.viaempresa.cat/es/opinion/ trabajo-derecho-genis-roca_2110488_102.xhtml>. <<

[61] Albert Cañigueral, *El trabajo ya no es lo que era*, Barcelona, Conecta, 2020. <<

[62] Ídem. <<

[63] Tal y como recomienda el Consejo Europeo. Véase «Recomendación del Consejo de 8 de noviembre de 2019 relativa al acceso a la protección social para los trabajadores por cuenta ajena y por cuenta propia», *Diario Oficial de la Unión Europea* (2019); disponible en <https://eur-lex. europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019 H1115(01)&from=EN>. <<

[64] Como sugiere la Universal Worker Protections Act del estado de Washington (Estados Unidos), 2019; disponible en <http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5690.pdf?q=20210309111340>. <<

[65] José María Lassalle, *Ciberleviatán*, Barcelona, Arpa, 2019. <<

[66] Como propone Jamie Bartlett, *The People vs Tech. How the Internet is Killing Democracy (and How We Save It)*, Nueva York, Penguin Random House, 2018. <<

[67] Algunas de estas propuestas están basadas en las recomendaciones del *think tank* Council on Foreign Relations (CFR). Véase nota 11 de este capítulo. <<

[68] Bruce Schneier, *Haz clic aquí para matarlos a todos. Un manual de supervivencia*, trad. de Álvaro Robledo, Barcelona, Temas de Hoy, 2019. <<

[69] Fragmento del artículo 5 del Tratado de Washington, el tratado fundacional de la OTAN (1949); disponible en <https://www.nato.int/cps/en/natolive/official_texts_17120.htm>. <<

[70] Véase nota 2, cap. 3. <<

[71] Schneier, *Haz clic aquí para matarlos a todos*… <<

[72] Según el informe «European Digital Sovereignty», Oliver Wyman, 2020. <<

[73] Como explica Adam Smith, consultor de servicios en la nube, soberanía digital y ciberseguridad en HiSolutions AG y asesor de Gaia-X, entrevistado el 8 de marzo de 2021. <<

[74] Según los datos de Statista del último cuatrimestre de 2020, <https://cdn.statcdn.com/Infographic/images/normal/18819.jpeg>. <<

[75] Steve Lohr, «He Created the Web. Now He’s Out to Remake the Digital World», *The New York Times* (2021); disponible en <https://www.nytimes.com/2021/01/10/technology/tim-berners-lee-privacy-internet.xhtml>. <<

[76] Según el propio Evan Henshaw-Plath, entrevistado el 13 de marzo de 2021. <<

[77] Ethan Zuckerman, «The Case for Digital Public Infrastructure Harnessing past successes in public broadcasting to build communityoriented digital tools», Knight First Amendment Institute, Universidad de Columbia, 2020; disponible en <https://s3.amazonaws.com/kfaidocuments/documents/7f5fdaa8d0/Zuckerman-1.17.19-FINAL-.pdf>.

[78] Como sugiere también James Williams. Véase nota 52 de este capítulo. << <<

[79] Como constata Mariana Mazzucato en *Faster than the future. Facing the digital age*, Barcelona, Digital Future Society (DFS), 2021. <<

[80] Extracto del discurso de Tim Cook durante la conferencia CPDP (Computers, Privacy and Data Protection) del 3 de febrero de 2021; disponible en <https://youtu.be/OaLxTz1Yw7M>. <<

[81] Véase nota 79 de este capítulo. <<

[82] Como propone Gemma Galdon Clavell (véase nota 10 de este capítulo); «Directiva 2010/75/UE del Parlamento Europeo y del Consejo de 24 de noviembre de 2010 sobre las emisiones industriales (prevención y control integrados de la contaminación)», *Diario Oficial de la Unión Europea* (2010); disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/ PDF/?uri=CELEX:32010L0075&from=EN>. <<

[83] Tal y como propone Simona Levi, dramaturga y cofundadora del colectivo Xnet por la cultura libre, experta en tecnopolítica y derechos digitales, entrevistada en varias ocasiones en noviembre de 2020. <<

[84] Son opciones que proponen expertos como James Williams o Ethan Zuckerman. Este último sugiere que la financiación provenga de un impuesto a la publicidad *online* altamente invasiva de la personalidad, pero, si esta se prohíbe, un impuesto así no será necesario. <<

[85] En alusión al «bote salvavidas» con el que Dan Dennett (entrevistado el 26 de junio de 2020) hace referencia a los refugios «absorbedores de pánico» ante una catástrofe como una caída masiva y prolongada de internet. Son lugares obvios a los que acudir ante un suceso de este tipo —como, por ejemplo, una iglesia—. También se refiere a la necesidad de cohesión social, solidaridad, colaboración y coordinación. <<

[1] Carlota Pérez, *Technological Revolutions and Financial Capital. The Dynamics of Bubbles and Golden Ages*, Londres, Edward Elgar, 2002. [Hay trad. cast.: *Revoluciones tecnológicas y capital financiero. La dinámica de las grandes burbujas financieras y las épocas de bonanza*, trad. de Nydia Ruiz, México, Siglo XXI, 2002.] <<

[2] Azeem Azhar entrevista a Carlota Pérez en su *podcast* «Exponential View with Azeem Azhar: Bubbles, Golden Ages, and Tech Revolutions» (temporada 4, episodio 3), *Harvard Business Review* (2019) ; disponible en <https://hbr.org/podcast/2019/10/bubbles-golden-ages-and-techrevolutions>. <<

[3] Dana Kanze, Mark A. Conley y E. Tory Higgins, «Research. Organizations That Move Fast Really Do Break Things», *Harvard Business Review* (2020); disponible en <https://hbr.org/2020/02/researchorganizations-that-move-fast-really-do-break-things>. <<

[4] Según muestran los datos del informe «Sustainable Funds U. S. Landscape Report», Morningstar, 2021; disponible en <https://www.morningstar.com/lp/sustainable-funds-landscape-report>. <<

[5] «Wall Street will soon have to take millennial investors seriously», *The Economist* (2021); disponible en <https://www.economist.com/ finance-and-economics/2020/10/20/wall-street-will-soon-have-to-takemillennial-investors-seriously>. <<

[6] Como muestran diversos análisis y estudios. Véanse «The new rules of competition in the technology industry»,*The Economist* (2021); disponible en <https://www.economist.com/business/2021/02/27/the-new-rulesof-competition-in-the-technology-industry>; Shira Ovide, «Tech Is Global. Right?», *The New York Times* (2021); disponible en <https://www.nytimes.com/2020/06/04/technology/internet-global-competition.xhtml>, y Casey Newton, «How social networks got competitive again Facebook's surprising new challengers in audio, video, photos, and text», *Platformer* (2021); disponible en <https://www.platformer.news/p/how-social-networksgot-competitive>. <<

[7] Albert Cañigueral, *El trabajo ya no es lo que era*, Barcelona, Conecta, 2020. <<

[*] La inteligencia artificial (IA) es un conjunto de técnicas informáticas avanzadas que intentan funcionar como el cerebro humano para procesar grandes volúmenes de datos de forma compleja y llevar a cabo tareas como detectar patrones, realizar recomendaciones y asistir en la toma de decisiones. <<

[*] El protocolo BGP o Border Gateway Protocol es la base del funcionamiento de internet. Sirve para enrutar el tráfico en la red de redes. Es decir, decide cómo viajan los datos de un lugar a otro en internet. <<

[*] No todos los *hackers* son malos. A los que sí lo son se les llama *crackers*. Como señala la FundéuRAE, a pesar de que a menudo emplee el término *hacker* para referirse a piratas informáticos maliciosos, un *hacker* es simplemente «una persona capaz de introducirse en sistemas informáticos ajenos». Un *cracker*, sin embargo, es el que «lo hace con fines ilícitos».

La gente pregunta a menudo: «¿Cuál será la próxima COVID?». Un ataque a nuestra infraestructura digital es uno de los principales candidatos. El coronavirus tardó varios meses en propagarse por el mundo e infectar a millones de personas. Nuestra infraestructura digital podría colapsar en un solo día. <<

[*] Un ataque de denegación de servicio distribuido o DDoS (Distributed Denial of Service) es lo que sus siglas en inglés indican: un ataque dirigido a «denegar» el servicio (o colapsar, o inhabilitar) de un servidor o de una infraestructura. Es «distribuido» porque se realiza desde múltiples fuentes que envían un número tan alto de solicitudes al sistema objetivo que este se sobrecarga. <<

[*] Estos sesgos hacen —según Kahneman— que tengamos percepciones prejuiciosas o distorsionadas. <<

[*] Creadores de contenido en la plataforma YouTube, que eventualmente consiguen cierta fama o incluso se convierten en celebridades. Son muy populares entre niños y adolescentes. <<

[**] En este contexto, personas con influencia *online*, que marcan tendencias en redes sociales (especialmente en aquellas dominadas por el contenido audiovisual, como Instagram) o en plataformas como YouTube. <<

[*] Mi amigo Javier Romañach, referente en la lucha por los derechos de las personas con discapacidad, solía decir que todos tenemos alguna discapacidad. Por eso este colectivo reivindica hablar simplemente de «personas con capacidades diferentes». <<

[**] A quien todo esto le resulte demasiado desalentador puede dirigirse a la parte final de este libro (la tercera), en la que propongo formas de abordarlo y casos de los que te reconcilian con el *Homo sapien*s. <<

[*] Es importante notar que «discriminar» no es *per se* algo negativo, sino todo lo contrario: es necesario. Vemos, por una parte, que varias acepciones de término aluden a esta como una forma de seleccionar; una capacidad para juzgar si algo es bueno o adecuado, de reconocer la diferencia entre las cosas (<https://www.mac millandictionary.com/dictionary/british/discrimination>). Por otra parte, significa también «dar trato desigual a una persona o colectividad por motivos raciales, religiosos, políticos, de sexo, de edad, de condición física o mental, etcétera» (<https:// dle.rae.es/discriminar>). A esta última acepción es a la que me refiero cuando hablo de «discriminación» en este capítulo. <<

[*] Sobre ello hablaremos más extensamente en el capítulo siguiente. <<